รายงานสรุปผลการอบรม

ชื่อโครงการฝึกอบรม : โครงการพัฒนาบุคลากรด้านคอมพิวเตอร์และสารสนเทศ

หลักสูตร “การสร้างความมั่นคงปลอดภัยทางไซเบอร์”

วันที่เข้ารับการอบรม : ๑๖ – ๑๗ พฤษภาคม ๒๕๖๗

สถานที่ : ห้องปฏิบัติการฝึกอบรมคอมพิวเตอร์และภูมิสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

จัดโดย : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ผู้จัดทำรายงาน : นางสาววิภา เอี่ยมพรรัตน์ ตำแหน่ง นักวิชาการเงินและบัญชีชำนาญการ

วัตถุประสงค์

๑. เพื่อให้เกิดความตระหนักรู้ในความมั่นคงปลอดภัยทางไซเบอร์

๒. เพื่อให้สามารถรับมือกับภัยคุกคามที่จะเกิดขึ้นได้อย่างปลอดภัย และแก้ปัญหาเบื้องต้นได้อย่างถูกต้อง

๓. เพื่อให้สามารถประเมินความเสี่ยงด้านไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน โดยมีแนวทางปฏิบัติที่ถูกต้องเหมาะสม

๔. เพื่อให้เกิดความรู้ความเข้าใจและตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคลของผู้รับบริการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

สรุปเนื้อหาการฝึกอบรม :

เจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เพื่อกำหนดให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพในการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจากการถูกล่วงละเมิด มิให้มีการกระทำได้โดยง่าย รวมทั้งกำหนดให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิ

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

๑. **เจ้าของข้อมูลส่วนบุคคล (Data Subject)**

๒. **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๓. **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามค าสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลประกอบด้วย

๑. **ข้อมูลที่ระบุตัวตนของบุคคล** เช่น ชื่อ – นามสกุล , ชื่อเล่น , เลขบัตรประจำตัวประชาชน , เลขหนังสือเดินทาง , เลขบัตรประกันสังคม , เลขใบอนุญาตขับขี่ , เลขประจำตัวผู้เสียภาษี , เลขบัญชีธนาคาร , เลขบัตรเครดิต , ที่อยู่ , อีเมล์ , เลขโทรศัพท์ , IP address MAC address , Cookie ID

๒. **ข้อมูลระบุทรัพย์สินของบุคคล** เช่น ทะเบียนรถยนต์ , โฉนดที่ดิน

๓. **ข้อมูลการประเมินผลการทำงาน** หรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

๔. **ข้อมูลทางชีวมิติ** เช่น รูปภาพใบหน้า , ลายนิ้วมือ , ฟิล์มเอกซเรย์ , ข้อมูลสแกนม่านตา , ข้อมูลอัตลักษณ์เสียง , ข้อมูลพันธุกรรม

๕. **ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้** เช่น วันเกิดและสถานที่เกิด , เชื้อชาติ , สัญชาติ , น้ำหนัก , ส่วนสูง , ข้อมูลตำแหน่งที่อยู่ , ข้อมูลการแพทย์ , ข้อมูลการศึกษา , ข้อมูลทางการเงิน , ข้อมูลการจ้างงาน

๖. **ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล** เช่น log file ข้อมูลอื่น ๆ ที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ห้ามเก็บรวมรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล **<u>เว้นแต่</u>**

๑. ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

๒. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

๓. เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มรวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน

๔. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๕. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๖. เป็นการจำเป็นในการปฏิบัติตามกฎหมาย

เจตนารมณ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

เพื่อให้มีมาตรการ ป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงกข่ายของหน่วยงานโครงสร้างพื้นฐานสำคัญ จนไม่สามารถทำงานได้เป็นปกติ อันกระทบต่อการให้บริการแก่ประชาชน ความมั่นคงของรัฐ หรือความสงบเรียบร้อยภายในประเทศ

พรบ.ไซเบอร์มีผลบังคับใช้กับ ๓ หน่วยงาน คือ

๑. หน่วยงานของรัฐ

- ราขการส่วนกลาง
- ราชการส่วนภูมิภาค
- ราชการส่วนท้องถิ่น
- รัฐวิสาหกิจ
- องค์กรฝ่ายนิติบัญญัติ
- องค์กรฝ่ายตุลาการ
- องค์กรอิสระ
- องค์การมหาชน
- หน่วยงานอื่นของรัฐ

๒. หน่วยงานควบคุมหรือกำกับดูแล

หน่วยงานของรัฐ หน่วยงานเอกชนหรือบุคคลหรือบุคคลซึ่งมีกฎหมายกำหนด ให้มีหน้าที่และอำนาจในการควบคุม หรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ: CII

ภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนทศ จัดกลุ่มได้เป็น ๘ ประเภท คือ

- ด้านความมั่นคงของรัฐ
- ด้านบริการภาครัฐที่สำคัญ
- ด้านการเงินการธนาคาร
- ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- ด้านการขนส่งและโลจิสติกส์
- ด้านพลังงานและสาธารณูปโภค
- ด้านสาธารณสุข
- หน่วยงานด้านอื่น ตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

ความหมายและคำนิยาม

๑. ไซเบอร์ (Cyber)

หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจาการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๒. ภัยคุกคามทางไซเบอร์ (Cyber Threat)

หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ ได้แก่

- **Virus** เป็นมัลแวร์ที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในเครื่องคอมพิวเตอร์
- **Worm** เป็นมัลแวร์ที่สามารถคัดลอกตัวเองและส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยช่องโหว่ของระบบปฏิบัติการ
- **Trojan** เป็นมัลแวร์ที่ต้องอาศัยการหลอกเหยื่อให้ดาวน์โหลดเอาไปใส่เครื่องเองแล้วคอยดักจับข้อมูลหรือทำลายข้อมูลเครื่อง
- **Spyware** ซอฟต์แวร์ที่ออกแบบเพื่อสังเกตการณ์ หรือดักจับข้อมูล หรือควบคุมเครื่องคอมพิวเตอร์
- **Sniffing** การดักรับข้อมูล โดยการดักจับการรับส่งข้อมูลเครือข่าย เมื่อข้อมูลถูกสั่งผ่านเครือข่าย
- **Spam** การส่งข้อความที่ผู้รับไม่ได้ร้องขอ ผ่านทางระบบอิเล็กทรอนิกส์ เช่น การส่งแสปมผ่านทางอีเมลในการโฆษณาชวนเชื่อ หรือโฆษณาขายของ
- **Phishing** การหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมล หรือแมสเซนเจอร์
- **Social Engineering** จิตวิทยาในการหลอกลวง เพื่อให้เหยื่อดำเนินการหรือเปิดเผยข้อมูลที่เป็นความลับ
- **Ransomware** เป็นมัลแวร์ที่สามารถบล็อกการเข้าถึงไฟล์ของเหยื่อ (เข้ารหัส) และวิธีเดียวที่จะได้รับสิทธิ์ในการเข้าถึงไฟล์คือ จ่ายค่าไถ่
- **Keylogger** เป็นมัลแวร์ที่เก็บทุกแป้นพิมพ์ที่ผู้ใช้พิมพ์ ทำการเก็บข้อมูลการใช้งานต่าง ๆ ของเครื่องที่ถูกติดตั้ง แล้วส่งไปยังแฮกเกอร์ (ส่วนใหญ่ Capture หน้าจอไปพร้อม ๆ กันด้วย) โดยไม่รู้ตัว
- **Botnet** เป็นมัลแวร์ชนิดหนึ่งที่อาศัยอินเทอร์เน็ตที่เข้าไปเชื่อมต่อกับคอมพิวเตอร์เป้าหมาย เพื่อควบคุมการทำงาน
- **Dos/Ddos** การพยายามโจมตีระบบคอมพิวเตอร์ ทำให้ไม่สามารถให้บริการได้

๓. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

๔. เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident)

หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหาย หรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๕. มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

หมายความว่า การแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๖. หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ

หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมรภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๗. โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานภาครัฐ หรือหน่วยงานภาคเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

การป้องกันการโจมตีทางไซเบอร์

๑. ใช้งานผ่าน HTTPS เท่านั้น

๒. ไม่ควรบันทึก Password ต่าง ๆ บน Browser

๓. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome , Mozilla Firefox เป็นต้น

๔. ไม่คลิกลิงค์ที่แนบมาใน E-Mail ของคนที่เราไม่รู้จัก ถ้าต้องการเข้าถึงเว็บไซต์นั้นจริง ๆ ให้พิมพ์ url ด้วยตัวเอง

๕. ควรมีการ Updater Version ของ Browser อย่างสม่ำเสมอ

ประโยชน์ที่ได้รับ

๑. ได้ความรู้และความเข้าใจ และตระหนักถึงความเสี่ยงจากการใช้งานข้อมูลส่วนบุคคลของผู้รับบริการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. ได้เรียนรู้ และเข้าใจเกี่ยวกับการดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์

๓. สามารถประเมินความเสี่ยงด้านไซเบอร์ภายในหน่วยงานได้ และมีแนวทางการดำเนินการที่ถูกต้องและเหมาะสม

๔. สามารถรับมือกับภัยคุกคามและแก้ปัญหาเบื้องต้นได้อย่างถูกต้อง