สรุปบทเรียนการพัฒนาความรู้

หลักสูตร

“การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)”

****

ชื่อ-สกุล (ภาษาไทย) นางสาวปราณี จอมอุ่น ตำแหน่ง นักวิทยาศาสตร์ชำนาญการ

สังกัด กลุ่มวิจัยกายภาพดิน สำนักวิทยาศาสตร์เพื่อการพัฒนาที่ดิน

วันที่อบรม 14 มิถุนายน 2566

วัตถุประสงค์ของหลักสูตร

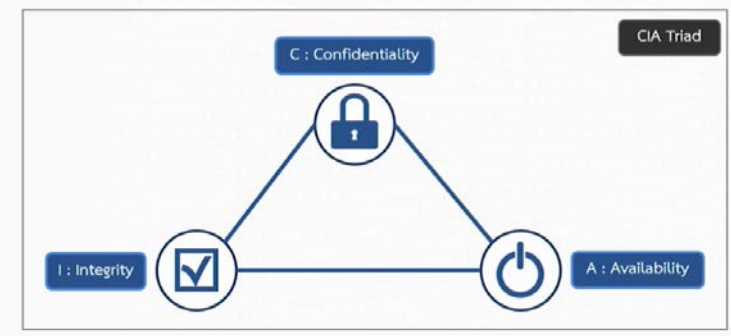
1. เพื่อให้ตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
2. เพื่อให้มีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
3. เพื่อนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

สรุปบทเรียน

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ตัวอย่างกฎหมายและมาตรการที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ เช่น พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

พื้นฐานของหลักการปฏิบัติเพื่อความปลอดภัยทางไซเบอร์ คือ CIA Triad



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ตามลำดับชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัทจัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

✎ Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน (ข้อมูลบัญชีธนาคาร)

✎ Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลบัญชีธนาคาร

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

- ☐ Computer
- ☐ Website
- ☐ Fake News
- ☐ Line Official Account
- ☐ Cloud Storage

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับตัวเองและองค์กร ดังนี้

<u>สำหรับบุคคล</u>

- ◈ ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์ที่ไม่มีการตรวจสอบแน่ชัดหรือเปิดไฟล์จาก บุคคลที่ไม่รู้จัก และระมัดระวังการเปิดไฟล์ผ่าน Social Media ทั้งนี้เพื่อหลีกเลี่ยงพวกมัลแวร์
- ◈ ไม่ใช้รหัสผ่านบน โลก cyber เป็นรหัสชุดเดียวกันทุกระบบ
- ◈ ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และพิจารณาข้อมูลก่อนการแชร์ข้อมูลต่อเพื่อป้องกัน ตนเองเป็นต้นตอ ต่อการส่งแพร่กระจายไวรัส

<u>สำหรับหน่วยงาน</u>

- ◈ ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและข้อมูล
- ◈ เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของไวรัส Web Application Firewall หรือ DDos Protection
- ◈ แจ้งเจ้าหน้าที่ของหน่วยงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงความเหมาะสมป้องกัน ข้อความจาก Social Media
- ◈ หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้าปกติ ควรตรวจสอบการ login ย้อนหลังทุกๆ เดือน
- ◈ ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ต่างๆ ตามที่กฎหมายกำหนดไว้

ประโยชน์ที่ได้รับต่อตนเอง

มีความรู้ ความเข้าใจให้สามารถป้องกันและเรียนรู้ว่าพฤติกรรมแบบไหนที่เสี่ยงต่อการเกิดการคุกคามทางไซเบอร์ เพื่อปกป้องทรัพย์สินและข้อมูลของตนเองให้ปลอดภัยไม่ให้ตกเป็นเหยื่อของมิจฉาชีพได้

ประโยชน์ที่ได้รับต่อหน่วยงาน

บุคลากรที่มีความรู้ด้านการรักษาความมั่นคงปลอดภัย สามารถใช้งานทรัพยากรสารสนเทศ ขององค์กรได้ถูกต้อง ปลอดภัย ป้องกันภัยคุกคามและแจ้งเหตุผิดปกติให้องค์กรสามารถยับยั้ง ความเสียหายได้ทันท่วงที เกิดความเชื่อมั่นด้านความปลอดภัย ผู้ใช้บริการและคู่ค้าทางธุรกิจจะไว้วางใจที่จะทำงานร่วมกับองค์กรของคุณมากขึ้น