ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

ชื่อ-นามสกุล น.ส.อาภัสนันท์ สุดเจริญ ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ กองเทคโนโลยีชีวภาพทางดิน

ที่มา: อบรมผ่านระบบออนไลน์ วันที่ 1 เดือน สิงหาคม 2569 จัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

วิทยากร 1. ดร.ปรัชญ์ สง่างาม สาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

2. ผศ.ดร.ทวีศักดิ์ สมานชื่น สาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

3. ผศ.ดร.โษฑศ์รัตต ธรรมบุษดี สาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

4. อาจารย์มนัสศิริ จันสุทธิรางกูร สาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

ในยุคปัจจุบันที่เทคโนโลยีสารสนเทศและการสื่อสารดิจิทัลได้เข้ามามีบทบาทสำคัญในการดำเนินชีวิตและการทำงาน การมีความรู้ความเข้าใจเกี่ยวกับบรรทัดฐานทางสังคมและข้อบังคับทางกฎหมายจึงเป็นสิ่งจำเป็นอย่างยิ่ง รวมไปถึงการปรับตัวเข้าสู่วิถีชีวิตดิจิทัลและการตระหนักรู้ด้านความปลอดภัยไซเบอร์ เพื่อส่งเสริมให้เกิดการใช้เทคโนโลยีอย่างมีความรับผิดชอบ ปลอดภัย และสร้างสรรค์ในสังคมดิจิทัล โดยมีรายละเอียด ดังนี้

1. กรอบจริยธรรมการใช้คอมพิวเตอร์และสารสนเทศ (PAPA Framework) หลักจริยธรรมพื้นฐาน 4 ประการ ที่ผู้ใช้และผู้บริหารจัดการเทคโนโลยีสารสนเทศต้องพิจารณา ดังนี้

1.1 ความเป็นส่วนตัว (Information Privacy) เช่น สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น และการละเมิดที่พบบ่อย เช่น แอบอ่าน E-mail การตรวจจับการทำงานของพนักงาน และแอบรวบรวมข้อมูลส่วนบุคคลไปขาย ฯลฯ

1.2 ความถูกต้อง (Information accuracy) เช่น ความน่าเชื่อถือและความถูกต้องของข้อมูล ซึ่งขึ้นอยู่กับการบันทึกข้อมูล และต้องมีผู้รับผิดชอบด้านความถูกต้องอย่างชัดเจน และตรวจสอบก่อนบันทึก

1.3 ความเป็นเจ้าของ (Intellectual Property) ได้แก่ สิ่งที่จับต้องได้ สิ่งที่จับต้องไม่ได้ การคุ้มครองตามกฎหมาย ลิขสิทธิ์ และสิทธิบัตร

1.4 การเข้าถึงข้อมูล (Data accessibility) ได้แก่ การกำหนดสิทธิในการเข้าถึงข้อมูลข่าวสารของผู้ใช้งาน กำหนดระดับสิทธิใช้งาน (Access rights) ให้เหมาะสม และออกแบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

2. บัญญัติ 10 ประการของการใช้อินเทอร์เน็ต ได้แก่

2.1 ไม่ใช้คอมพิวเตอร์ทำร้ายหรือละเมิดผู้อื่น (ไม่สร้างความเสียหาย รบกวน หรือกลั่นแกล้งผู้อื่น)

2.2 ไม่รบกวนการทำงานของผู้อื่น (ไม่ส่งไฟล์รบกวน ปล่อยไวรัส หรือก่อความรำคาญ)

2.3 ไม่สอดแนม แก้ไข หรือเปิดดูแฟ้มข้อมูลผู้อื่น (เคารพความเป็นส่วนตัวของไฟล์และข้อมูลบุคคลอื่น)

2.4 ไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูล (ไม่ขโมยข้อมูล ข่าวสาร หรือทรัพย์สินทางปัญญา)

2.5 ไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ (ไม่สร้างข่าวปลอม ปลอมแปลงเอกสาร หรือหลอกลวง

2.6 ไม่คัดลอกโปรแกรมของผู้อื่นที่มีลิขสิทธิ์ (ไม่ใช้ซอฟต์แวร์เถื่อน หรือทำซ้ำซอฟต์แวร์โดยไม่ได้รับอนุญาต)

2.7 ไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์ (ไม่แอบใช้เครื่อง Server หรือ Bandwidth ที่ตนเองไม่มีสิทธิ์)

2.8 ไม่นำเอาผลงานของผู้อื่นมาเป็นของตน (ไม่ทำ Plagiarism ลอกเลียนผลงานหรือแอบอ้างงานผู้อื่น)

2.9 คำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคม (ตระหนักถึงผลลัพธ์ของโปรแกรมหรือเนื้อหาที่สร้างขึ้นต่อส่วนรวม)

2.10 เคารพกฎ ระเบียบ กติกา และมีมารยาท (ปฏิบัติตนเป็นพลเมืองดิจิทัลที่ดี (Digital Citizen))

3. กฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา

3.1 การแบ่งประเภททรัพย์สินทางปัญญา

3.1.1 ทรัพย์สินทางอุตสาหกรรม (Industrial Property) ได้แก่ สิทธิบัตร (Patents) เครื่องหมายการค้า (Trademarks) การออกแบบอุตสาหกรรม (Industrial Designs) และสิ่งบ่งชี้ทางภูมิศาสตร์ (Geographic Indications)

3.1.2 ลิขสิทธิ์ (Copyright) เช่น งานวรรณกรรมและศิลปกรรม นิยาย บทกวี บทละคร ภาพยนตร์ ดนตรีกรรม ภาพเขียน ภาพถ่าย ประติมากรรม สถาปัตยกรรม และโปรแกรมคอมพิวเตอร์

3.2 ลักษณะสำคัญของลิขสิทธิ์

3.2.1 สิทธิแต่เพียงผู้เดียว (Exclusive rights) โดยเจ้าของลิขสิทธิ์มีสิทธิทำซ้ำ ดัดแปลง เผยแพร่ หรือให้เช่าแต่เพียงผู้เดียว

3.2.2 คุ้มครองการแสดงออกของความคิด (Expression of Ideas) ได้แก่ คุ้มครองรูปแบบงานที่ถ่ายทอดออกมาแล้ว ไม่คุ้มครองตัวความคิดที่ยังไม่ได้ถ่ายทอดออกมา

3.2.3 ความคิดริเริ่มของตนเอง (Originality) ไม่จำเป็นต้องมีความใหม่สด (Novelty) ขอเพียงเกิดจากความคิดริเริ่มของตนเอง (Original)

3.2.4 ระยะเวลาคุ้มครองยาวนาน โดยทั่วไปคุ้มครองตลอดอายุผู้สร้างสรรค์ จนถึง 50 ปี หลังเสียชีวิต (ยาวนานกว่าสิทธิบัตรที่มีอายุ 20 ปี)

3.3 สิทธิทางเศรษฐกิจ (Economic rights)

3.3.1 ทำซ้ำและดัดแปลง ได้แก่ การคัดลอก เลียนแบบ ทำสำเนา บันทึกภาพหรือเสียง หรือปรับปรุงแก้ไขงานต้นฉบับ

3.3.2 เผยแพร่ต่อสาธารณชน ได้แก่ นำงานออกแสดง บรรยาย สตรีมมิ่ง จำหน่าย หรือทำให้ปรากฏด้วยภาพหรือเสียง

3.3.3 ให้เช่า ได้แก่ สิทธิให้เช่าต้นฉบับหรือสำเนาของโปรแกรมคอมพิวเตอร์ โสตทัศนวัสดุ ภาพยนตร์ และสิ่งบันทึกเสียง

3.3.4 อนุญาตให้ผู้อื่นใช้สิทธิ ได้แก่ กำหนดเงื่อนไขการใช้สิทธิได้ แต่ต้องไม่เป็นการจำกัดการแข่งขันอย่างไม่เป็นธรรม

4. สื่อดิจิทัล และความปลอดภัย

4.1 สื่อดิจิทัล (Digital Media) สื่อที่นำเอาข้อความ กราฟิก ภาพเคลื่อนไหว และเสียง มาจัดรูปแบบโดยอาศัยเทคโนโลยีคอมพิวเตอร์และการสื่อสาร ช่วยลดต้นทุนและระยะเวลาในการทำงานลงอย่างมาก

4.2 ความปลอดภัยและภัยคุกคามในยุคดิจิทัล (Cyber Security) ได้แก่

4.2.1 รอยเท้าดิจิทัล (Digital Footprint) ได้แก่ ประวัติการกระทำ การโพสต์ หรือข้อมูลที่เราทิ้งไว้บนโลกออนไลน์ ซึ่งจะคงอยู่และอาจถูกนำมาใช้ประเมินหรือส่งผลกระทบต่อเราในอนาคต

4.2.2 ภัยคุกคามไซเบอร์ ได้แก่ การแบล็คเมล์ (Blackmail) ด้วยสื่อลามกหรือภาพหลุด ซึ่งผลการวิจัยพบว่าทั้งชายและหญิงมีโอกาสตกเป็นเหยื่อพอๆ กัน

4.2.3 การป้องกัน ทำได้โดยการระมัดระวังการเปิดเผยข้อมูลส่วนบุคคล การตั้งรหัสผ่านที่รัดกุม และการตรวจสอบสิทธิเข้าถึงระบบ