แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ด้วย นายธิปไตย ไตรโภค ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัด กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ หลักสูตร "Digital Literacy : ความฉลาดทางดิจิทัล (Digital Intelligence)" วันที่ ๒ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๐ นาที หลักสูตรดังกล่าวจัดโดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิตัล (TDGA)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์

๑. เพื่อให้ผู้เรียนเข้าใจความหมาย และเห็นความสำคัญ การสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต

๒. เพื่อให้ผู้เรียนมีความรู้การสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต รู้เท่าทัน และมีความมั่นคง ปลอดภัยเพื่อยกระดับวิถีชีวิตด้วยดิจิทัล

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

๒.๑ Digital Identity อัตลักษณ์ดิจิทัล

๒.๑.๑ โลกดิจิทัล (Digital World) คือ ระบบนิเวศของเทคโนโลยีที่เชื่อมโยงกันผ่านอินเทอร์เน็ต อุปกรณ์อิเล็กทรอนิกส์ และข้อมูลดิจิทัล ซึ่งเข้ามาเปลี่ยนวิธีการใช้ชีวิต การทำงาน และการสื่อสารของมนุษย์ให้รวดเร็วและไร้พรมแดน

๑) โลกดิจิทัลขับเคลื่อนด้วยองค์ประกอบหลัก ได้แก่:

- โครงสร้างพื้นฐาน: อินเทอร์เน็ตความเร็วสูง, เครือข่ายไร้สาย (๕G), และระบบคลาวด์ (Cloud Computing)
- อุปกรณ์ดิจิทัล: สมาร์ทโฟน, คอมพิวเตอร์, และอุปกรณ์ IoT (Internet of Things) ต่าง ๆ
- ข้อมูลและการประมวลผล: การใช้ AI และ Big Data เพื่อวิเคราะห์และตัดสินใจ
- แพลตฟอร์มและบริการ: โซเชียลมีเดีย, การทำธุรกรรมออนไลน์ (E-Commerce/E-Payment) และความบันเทิงดิจิทัล

๒) ผลกระทบและการเปลี่ยนแปลง

- การเข้าถึงข้อมูล: สามารถหาความรู้ และเรียนรู้ได้ทุกที่ทุกเวลา (Anytime, Anywhere) ผ่านช่องทางออนไลน์
- การเชื่อมต่อทางสังคม: ทลายขีดจำกัดด้านระยะทาง ทำให้ผู้คนทั่วโลกสามารถติดต่อสื่อสารกันได้ทันที
- เศรษฐกิจดิจิทัล: เกิดโมเดลธุรกิจใหม่ ๆ เช่น การขายของออนไลน์ และการทำงานแบบ Work from Anywhere

- การบริการภาครัฐ: มีความโปร่งใส และรวดเร็วขึ้นผ่านระบบดิจิทัล (E-Government) การใช้ Search Engine ให้เกิดประโยชน์สูงสุดนั้นต้องอาศัยเทคนิคบางอย่าง

๓) ข้อควรระวังและทักษะที่จำเป็น ในยุคนี้ บุคคลจำเป็นต้องมีทักษะ การรู้เท่าทันดิจิทัล (Digital Literacy) เพื่อรับมือกับความเสี่ยง:

- ภัยคุกคามทางไซเบอร์: การถูกแฮ็กข้อมูล, การหลอกลวงออนไลน์ (Phishing) และไวรัสคอมพิวเตอร์

- สุขภาพกายและจิต: ภาวะเสพติดหน้าจอ (Social Media Addiction), การบูลลี่ทางไซเบอร์ (Cyberbullying) และปัญหาออฟฟิศซินโดรม

- จริยธรรม: การเคารพสิทธิส่วนบุคคลและการใช้สื่ออย่างมีจรรยาบรรณ

๒.๑.๒ อัตลักษณ์ดิจิทัล (Digital Identity) คือ ข้อมูลหรือชุดลักษณะเฉพาะที่ระบุตัวตนของบุคคล องค์กร หรืออุปกรณ์ในโลกออนไลน์ เปรียบเสมือน "บัตรประชาชนเสมือน" ที่ช่วยให้เราสามารถยืนยันตัวตนเพื่อทำธุรกรรม หรือเข้าถึงบริการต่าง ๆ ผ่านอินเทอร์เน็ตได้อย่างปลอดภัยและน่าเชื่อถือ

๑) องค์ประกอบของอัตลักษณ์ดิจิทัล ข้อมูลที่ประกอบกันเป็นตัวตนในโลกดิจิทัล มีหลายประเภท ได้แก่:

- ข้อมูลส่วนตัว: ชื่อ-นามสกุล, วันเดือนปีเกิด, ที่อยู่, เลขบัตรประชาชน

- ข้อมูลชีวมิติ (Biometrics): ลายนิ้วมือ, การสแกนใบหน้า, ม่านตา

- ข้อมูลการใช้งาน: ชื่อผู้ใช้งาน (Username), รหัสผ่าน, อีเมล, ประวัติการเข้าชมเว็บ

- ข้อมูลอุปกรณ์: เลข IP Address, รหัสประจำเครื่อง (Device ID)

๒) ความสำคัญในโลกดิจิทัล

- การทำธุรกรรมออนไลน์: ใช้ในการเปิดบัญชีธนาคาร (E-KYC), โอนเงิน, ชำระสินค้า หรือกู้ยืมผ่านแอปพลิเคชัน

- บริการภาครัฐ: ช่วยให้ติดต่อหน่วยงานราชการได้โดยไม่ต้องเดินทาง เช่น การตรวจสอบสิทธิสวัสดิการหรือขอใบรับรองต่าง ๆ

- ความปลอดภัย: ป้องกันการสวมรอยหรือการฉ้อโกง (Fraud) โดยมีระบบตรวจสอบที่เป็นมาตรฐาน

- ความเป็นส่วนตัว: นวัตกรรมใหม่อย่าง Decentralized Digital Identity (DDI) ช่วยให้เจ้าของข้อมูลสามารถควบคุม และเลือกเปิดเผยข้อมูลของตนเองได้มากขึ้น

๓) ประโยชน์ที่ได้รับ

- ความสะดวก: ลดการใช้สำเนาเอกสารกระดาษและลดขั้นตอนการเดินทาง

- ความรวดเร็ว: ยืนยันตัวตนได้ทันทีผ่านสมาร์ทโฟน

- ความน่าเชื่อถือ: สร้างความมั่นใจให้แก่ผู้ให้บริการว่าผู้ใช้งานคือตัวจริง

๔) ข้อควรระวังและภัยคุกคาม เช่น:

- การถูกขโมยอัตลักษณ์ (Identity Theft): ผ่านการ Phishing, มัลแวร์ หรือการแฮ็กข้อมูล

- ความเป็นส่วนตัว: ข้อมูลพฤติกรรมการใช้งานอาจถูกจัดเก็บและนำไปใช้ในทางที่ไม่เหมาะสมหากไม่มีการกำกับดูแลที่ดี

๒.๑.๓ ความเป็นส่วนตัวในโลกดิจิทัล (Digital Privacy) คือ สิทธิในการควบคุมข้อมูลส่วนบุคคลของเราบนโลกออนไลน์ ไม่ว่าจะเป็นกิจกรรมการใช้งาน การสื่อสาร หรือข้อมูลที่ระบุตัวตนได้ โดยในปัจจุบัน ประเด็นนี้ได้ยกระดับจากการสร้างความตระหนักรู้ไปสู่ "การลงมือปฏิบัติจริง (Privacy in Action)" ที่เข้มข้นขึ้นทั้งในระดับบุคคลและองค์กร

๑) ขอบเขตของความเป็นส่วนตัวดิจิทัล ความเป็นส่วนตัวไม่ได้หมายถึงแค่ "ความลับ" แต่รวมถึงการจัดการข้อมูลใน ๓ ด้านหลัก:

- ความเป็นส่วนตัวของข้อมูลบุคคล (Individual Privacy): การปกป้องข้อมูลที่ระบุตัวตน เช่น เลขบัตรประชาชน ข้อมูลสุขภาพ และข้อมูลชีวมิติ

- ความเป็นส่วนตัวของข้อมูลการใช้งาน (Information Privacy): การควบคุมว่าเว็บไซต์หรือแอปพลิเคชันจะจัดเก็บและใช้ประวัติการเข้าชมเว็บ พฤติกรรมการซื้อสินค้า หรือตำแหน่งที่ตั้ง (Location) ของเราอย่างไร

- ความเป็นส่วนตัวของการสื่อสาร (Communication Privacy): การรักษาความลับของข้อความ อีเมล และการโทรผ่านแอปพลิเคชันไม่ให้ถูกดักฟัง หรือเข้าถึงโดยไม่ได้รับอนุญาต

๒) สถานการณ์ความเป็นส่วนตัว

- การบังคับใช้กฎหมายที่เข้มข้น: คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) เน้นการตรวจสอบและลงโทษอย่างจริงจัง โดยมีการสั่งปรับองค์กรที่ทำข้อมูลรั่วไหล หรือไม่มีมาตรการความปลอดภัยที่เพียงพอในอัตราที่สูงขึ้น

- ความท้าทายจาก AI: การเติบโตของ AI Agent ทำให้ข้อมูลส่วนบุคคลถูกนำไปวิเคราะห์ในระดับที่ลึกขึ้น และมีการนำ AI มาใช้สร้างกลโกงเพื่อเข้าถึงข้อมูลส่วนตัว (เช่น การปลอมหน้าและเสียง)

- ระบบเศรษฐกิจที่ขับเคลื่อนด้วยความเชื่อมั่น (Trust Ecosystem): ธุรกิจที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลจะได้รับความไว้วางใจจากลูกค้ามากขึ้น และกลายเป็นมาตรฐานสากลในการทำธุรกิจ

๓) วิธีปกป้องความเป็นส่วนตัวเบื้องต้น เพื่อให้รอดพ้นจากภัยคุกคามและการถูกติดตามในโลกดิจิทัล ควรปฏิบัติดังนี้:

- ตรวจสอบความยินยอม (Consent): ก่อนกด "ยอมรับ" ข้อตกลงการใช้งาน ควรสังเกตว่ามีการขอเข้าถึงข้อมูลที่เกินความจำเป็นหรือไม่

- จัดการรอยเท้าดิจิทัล (Digital Footprint): จำกัดการแชร์ข้อมูลส่วนตัวที่ระบุพิกัดเรียลไทม์ หรือกิจวัตรประจำวันบนโซเชียลมีเดีย

- ใช้เครื่องมือเสริมความปลอดภัย: เช่น การเข้ารหัสข้อมูล (Encryption), การยืนยันตัวตนหลายชั้น (MFA) และการใช้งาน VPN เมื่อต้องเชื่อมต่อเครือข่ายสาธารณะ

- ตรวจสอบลิงก์และไฟล์: ระวังการคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือเพื่อป้องกันการถูกขโมยข้อมูล (Phishing)

๒.๒ Digital Use การใช้เทคโนโลยีอย่างเหมาะสม-การใช้เทคโนโลยีอย่างสมดุล

๒.๒.๑ การใช้เทคโนโลยีอย่างสมดุล หรือ Digital Well-being คือการจัดสรรเวลาและวิธีการใช้เทคโนโลยีให้เกิดประโยชน์สูงสุด โดยไม่ให้ส่งผลเสียต่อสุขภาพกาย ใจ และความสัมพันธ์รอบตัว

๑) สร้างสมดุล เพราะการเสพติดหน้าจอ (Screen Addiction) นำมาซึ่งปัญหาหลายอย่างดังนี้

- สุขภาพกาย: ปวดตา (Computer Vision Syndrome), นิ้วล็อก, ออฟฟิศซินโดรม และการนอนหลับไม่มีคุณภาพ
- สุขภาพจิต: ภาวะสมาธิสั้น ความเครียดจากการเปรียบเทียบชีวิตในโซเชียล และความเหนื่อยล้าทางข้อมูล (Information Overload)
- ความสัมพันธ์: "สังคมก้มหน้า" ทำให้การสื่อสารกับคนตรงหน้าลดลง

๒) แนวทางปฏิบัติเพื่อความสมดุล

- Digital Detox: กำหนดเวลา "พักหน้าจอ" เช่น งดใช้มือถือหลัง ๓ ทุ่ม หรือช่วงรับประทานอาหาร
- จัดการการแจ้งเตือน: ปิด Notification ที่ไม่จำเป็นเพื่อลดการถูกดึงดูดความสนใจโดยไม่ตั้งใจ
- กฎ ๒๐-๒๐-๒๐: เพื่อถนอมสายตา ให้พักทุก ๒๐ นาที มองไปที่ไกล ๆ ๒๐ ฟุต เป็นเวลา ๒๐ วินาที
- คัดกรองเนื้อหา: เลือกเสพสื่อที่สร้างพลังบวก หรือความรู้ แทนการไถฟีดแบบไม่มีจุดหมาย

๓) เครื่องมือช่วยจัดการ ในปัจจุบันสมาร์ทโฟนมีฟีเจอร์ที่ช่วยเราได้มาก:

- Android Digital Wellbeing: ช่วยดูสถิติการใช้งาน และจำกัดเวลาใช้แอป
- Apple Screen Time: ตั้งค่าการใช้งานของตัวเองและคนในครอบครัว

๒.๒.๒ การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) คือความสามารถในการทำความเข้าใจและคำนึงถึงความรู้สึกของผู้อื่นเมื่อสื่อสารผ่านโลกออนไลน์ เนื่องจากเราไม่ได้เห็นหน้า หรือได้ยินเสียงกันโดยตรง จึงต้องระวังเป็นพิเศษ

๑) ความสำคัญ

- ลดความขัดแย้ง: การพิมพ์ข้อความมักขาดการรับรู้น้ำเสียง (Tone of Voice) ทำให้เกิดการตีความผิดได้ง่าย
- ป้องกันการกลั่นแกล้ง (Cyberbullying): การคิดก่อนโพสต์ช่วยลดการสร้างบาดแผลทางใจให้ผู้อื่น
- สร้างสังคมเชิงบวก: ช่วยให้โลกออนไลน์เป็นพื้นที่ที่ปลอดภัยและน่าอยู่สำหรับทุกคน

๒) หลักการปฏิบัติ "เอาใจเขามาใส่ใจเรา"

- คิดก่อนพิมพ์ (THINK Test): ก่อนโพสต์ หรือคอมเมนต์ ให้ถามตัวเองว่าสิ่งที่เขียนนั้น True (จริงไหม) Helpful (ช่วยอะไรไหม) Inspiring (สร้างสรรค์ไหม) Necessary (จำเป็นไหม) Kind (ใจดีหรือเปล่า)

- เคารพความแตกต่าง: ยอมรับว่าคนในโลกโซเชียลมีพื้นฐานและความคิดเห็นที่หลากหลาย ไม่ใช้ถ้อยคำหยาบคายหรือสร้างความเกลียดชัง (Hate Speech)

- ไม่ตัดสินเร็วเกินไป: เมื่อเห็นคนอื่นโพสต์ผิดพลาด ให้พยายามทำความเข้าใจบริบทก่อนจะตำหนิ หรือแชร์ต่อ

๓) การแสดงออกที่เหมาะสม

- ใช้สัญลักษณ์ช่วย: เช่น Emojis เพื่อสื่ออารมณ์ให้ชัดเจน ลดความแข็งกระด้างของข้อความ

- ให้เกียรติความเป็นส่วนตัว: ไม่แท็กรูปที่เพื่อนดูไม่ดี หรือไม่เปิดเผยข้อมูลส่วนตัวของคนอื่นโดยไม่ได้รับอนุญาต

๒.๓ Digital Security การจัดการความปลอดภัยในโลกดิจิทัล

การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security Management) ในปัจจุบันมุ่งเน้นไปที่การใช้เทคโนโลยีขั้นสูงเพื่อรับมือกับภัยคุกคามที่ซับซ้อนขึ้น โดยเฉพาะภัยที่ขับเคลื่อนด้วย AI สรุปเนื้อหาสำคัญได้ดังนี้

๒.๓.๑ แนวโน้มและกติกาใหม่

- ปีแห่งการป้องกันแบบอัตโนมัติ: เป็นยุคที่ระบบป้องกันต้องทำงานด้วย AI แบบอัตโนมัติ (Automated AI Defense) เนื่องจากเป็นวิธีเดียวที่สามารถต่อกรกับความเร็วของภัยคุกคามที่ใช้ AI โจมตีได้ทันท่วงที

- สถาปัตยกรรม Zero Trust: การไม่เชื่อถือใครเลยเป็นมาตรฐานหลัก (Standard) โดยต้องตรวจสอบตัวตนอย่างต่อเนื่อง ไม่ว่าจะเป็นผู้ใช้ภายในหรือภายนอกองค์กร

- การจัดการตัวตนของเครื่องจักร (Machine Identities): นอกจากการดูแลตัวตนบุคคลแล้ว ปัจจุบันการจัดการความปลอดภัยของ AI Agent และอุปกรณ์ IoT สำคัญมาก เพราะมีจำนวนมากกว่าตัวตนของมนุษย์

๒.๓.๒ มาตรการพื้นฐานที่ต้องทำให้เข้มงวด (Individual & Org Tips)

- การยืนยันตัวตนหลายชั้น (MFA): ยกระดับจากการใช้ SMS ไปสู่การใช้ MFA ที่ป้องกันการ Phishing ได้ เช่น การใช้กุญแจความปลอดภัย (Security Keys) หรือการพิสูจน์ตัวตนด้วยพฤติกรรม

- รหัสผ่านที่ยากต่อการคาดเดา: ตั้งรหัสให้ซับซ้อนและควรเปลี่ยนทุก ๓-๖ เดือน รวมถึงไม่ใช้รหัสซ้ำกันในหลายบริการ

- การอัปเดตระบบ (Patch Management): ควรให้ความสำคัญกับการอัปเดตช่องโหว่ที่มีการโจมตีจริง (Exploited) ทันที มากกว่าการรออัปเดตตามรอบเวลาปกติ

- สำรองข้อมูลแบบ Immutable: การสำรองข้อมูลต้องไม่สามารถถูกแก้ไข หรือลบได้ (Immutable Backup) เพื่อป้องกันการถูกเข้ารหัสจากมัลแวร์เรียกไถ่ (Ransomware)

๒.๓.๓ ข้อควรระวังในการใช้งาน

- ใส่ใจรอยเท้าดิจิทัล (Digital Footprint): ข้อมูลที่โพสต์ลงออนไลน์จะคงอยู่ตลอดไป แม้ลบแล้วก็อาจถูกสืบค้นย้อนหลังได้ จึงต้องระวังการเปิดเผยข้อมูลส่วนตัวและที่ตั้ง

- หลีกเลี่ยง Wi-Fi สาธารณะ: สำหรับธุรกรรมสำคัญ เช่น การเงินหรือการเข้าถึงระบบงาน ควรใช้เครือข่ายส่วนตัวหรือ VPN

- ระวัง Deepfakes และ Social Engineering: อาชญากรใช้ AI ปลอมแปลงเสียงและใบหน้าเพื่อหลอกลวง การตรวจสอบความน่าเชื่อถือก่อนโอนเงิน หรือให้ข้อมูลจึงเป็นเรื่องสำคัญที่สุด

๒.๓.๔ การกำกับดูแลและความเป็นส่วนตัว

- การบูรณาการความปลอดภัยและความเป็นส่วนตัว: องค์กรต้องรวมศูนย์การจัดการความปลอดภัยทางไซเบอร์เข้ากับนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy & Security Convergence) เพื่อให้สอดคล้องกับกฎหมายที่เข้มงวดขึ้น

๒.๔ Digital Literacy ด้านการรู้เท่าทันดิจิทัล

๒.๔.๑ การรู้เท่าทันดิจิทัล (Digital Literacy) ในด้านการใช้งานสื่อสารสนเทศ คือ ทักษะในการ "เข้าถึง วิเคราะห์ และสร้างสรรค์" ข้อมูลในโลกออนไลน์อย่างมีประสิทธิภาพและปลอดภัย สรุปประเด็นสำคัญได้ ดังนี้

๑) การเข้าถึงและสืบค้น (Access)

- การค้นหาที่ฉลาด: รู้วิธีใช้ Keyword เพื่อหาข้อมูลที่ต้องการได้รวดเร็วและแม่นยำ

- การคัดกรองแหล่งข้อมูล: เลือกใช้แหล่งข้อมูลที่มีความน่าเชื่อถือ เช่น เว็บไซต์ทางการของหน่วยงาน (.go.th, .or.th) หรือบทความวิชาการ

๒) การวิเคราะห์และประเมิน (Evaluate) สำคัญมากในการรับมือกับ ข่าวปลอม (Fake News) โดยต้องเช็กก่อนเชื่อผ่านหลักการ Source: ใครเป็นคนเขียน แหล่งข่าวมาจากไหน Date: ข้อมูลปัจจุบันหรือเปล่า (บางครั้งเป็นข่าวเก่าที่ถูกนำมาเล่าใหม่) Bias: เนื้อหามีอคติหรือพยายามปั่นหัวให้เราโกรธ/กลัวหรือไม่ Cross-check: ตรวจสอบจากหลายๆ แหล่งว่าพูดตรงกันไหม

๓) การสร้างสรรค์และสื่อสาร (Create & Communicate)

- การผลิตเนื้อหาที่มีคุณภาพ: สร้างสื่อที่ไม่ละเมิดลิขสิทธิ์ ไม่สร้างความเกลียดชัง (Hate Speech)

- มารยาทในโลกดิจิทัล (Netiquette): สื่อสารด้วยความสุภาพ เคารพความเป็นส่วนตัวของผู้อื่น และรู้จักกาลเทศะในการใช้สื่อแต่ละแพลตฟอร์ม

๔) การจัดการความปลอดภัยและลิขสิทธิ์

- ลิขสิทธิ์ดิจิทัล: เข้าใจเรื่องการอ้างอิงแหล่งที่มาและการใช้รูปภาพหรือเนื้อหาภายใต้สัญญาอนุญาต Creative Commons

- การปกป้องข้อมูล: ไม่แชร์ข้อมูลส่วนตัวที่อาจเป็นอันตรายและรู้วิธีจัดการกับสิทธิในข้อมูลของตนเอง

๒.๔.๒ การรู้เท่าทันดิจิทัลในบทบาท "ผู้จัดทำสื่อและสารสนเทศ" (Digital Content Creator)

๑) ความรับผิดชอบต่อเนื้อหา (Content Responsibility)

- ความถูกต้อง (Accuracy): ต้องตรวจสอบข้อเท็จจริง (Fact-check) ก่อนเผยแพร่ เพื่อไม่ให้เป็นต้นตอของข่าวปลอม (Fake News)

- ความเป็นกลางและไม่มีอคติ: นำเสนอข้อมูลที่สมดุล ไม่บิดเบือนเพื่อสร้างดราม่าหรือ Clickbait ที่เกินจริง

- การอ้างอิง (Citing Sources): ให้เกียรติแหล่งที่มาของข้อมูลเสมอ เพื่อสร้างความน่าเชื่อถือและโปร่งใส

๒) จริยธรรมและกฎหมายดิจิทัล

- ลิขสิทธิ์ (Copyright & Creative Commons): เข้าใจการใช้ทรัพย์สินทางปัญญาของผู้อื่น เลือกใช้สื่อที่เป็น Creative Commons หรือซื้อลิขสิทธิ์ให้ถูกต้อง

- การคุ้มครองข้อมูลส่วนบุคคล (PDPA): ไม่นำภาพหรือข้อมูลของผู้อื่นมาใช้ในสื่อโดยไม่ได้รับอนุญาต (Consent)

- การหลีกเลี่ยงประทุษวาจา (Hate Speech): ผลิตสื่อที่สร้างสรรค์ ไม่ยุยงให้เกิดความเกลียดชังหรือการบูลลี่ในสังคมออนไลน์

๓) การออกแบบสื่อเพื่อทุกคน (Inclusivity & Accessibility)

- Digital Inclusion: คำนึงถึงผู้ชมที่หลากหลาย เช่น การทำคำบรรยาย (Caption) สำหรับผู้บกพร่องทางการได้ยิน หรือการเลือกสีที่ไม่กระทบต่อผู้บกพร่องทางการมองเห็น

- User Experience (UX): จัดทำสารสนเทศให้อ่านง่าย เข้าใจง่าย และเข้าถึงได้สะดวกในทุกอุปกรณ์

๔) การใช้ AI อย่างมีจริยธรรม (AI Ethics in Content Creation)

- ความโปร่งใส (Transparency): หากใช้ AI ในการช่วยผลิตหรือตกแต่งภาพ/วิดีโอ ควรมีการระบุให้ชัดเจน เพื่อป้องกันการเข้าใจผิดว่าเป็นเหตุการณ์จริง (ลดปัญหา Deepfakes)

- การตรวจสอบผลลัพธ์จาก AI: ไม่เชื่อข้อมูลจาก AI ทั้งหมด ๑๐๐% ต้องมีการรีเช็กโดยมนุษย์เสมอ

๒.๕ Digital Communication ด้านการสื่อสารดิจิทัล

๒.๕.๑ ร่องรอยดิจิทัล (Digital Footprint) ในด้านการสื่อสาร คือ "รอยเท้า" หรือข้อมูลทุกอย่างที่คุณทิ้งไว้เมื่อใช้งานอินเทอร์เน็ต ซึ่งจะคงอยู่ตลอดไปและส่งผลต่ออนาคต

๑) ประเภทของร่องรอยดิจิทัล

- ร่องรอยที่ตั้งใจทิ้งไว้ (Active): ข้อมูลที่เราโพสต์เอง เช่น สเตตัสบนโซเชียล การคอมเมนต์ รูปภาพ หรือการส่งอีเมล

- ร่องรอยที่ไม่ได้ตั้งใจทิ้งไว้ (Passive): ข้อมูลที่ระบบเก็บอัตโนมัติ เช่น เลข IP Address ประวัติการค้นหา คุกกี้ (Cookies) ของเว็บไซต์ และพิกัดตำแหน่ง (Location)

๒) ทำไมเราต้องใส่ใจ

- ชื่อเสียงดิจิทัล (Digital Reputation) ในปัจจุบันบริษัทและมหาวิทยาลัยมักตรวจสอบ "รอยเท้า" ย้อนหลังเพื่อดูตัวตนที่แท้จริงก่อนรับเข้าทำงานหรือเข้าเรียน

- ความปลอดภัย: ร่องรอยที่มากเกินไปช่วยให้อาชญากรไซเบอร์เดารหัสผ่านหรือทำการหลอกลวง (Social Engineering) ได้ง่ายขึ้น

- ข้อมูลถาวร: แม้คุณจะกด "ลบ" แต่ข้อมูลอาจถูกแคปหน้าจอ หรือถูกบันทึกไว้ในระบบสำรอง (Server) ของแพลตฟอร์มไปแล้ว

๓) วิธีจัดการร่องรอยให้ดูดีและปลอดภัย

- คิดก่อนคลิก (Pause before Post)

- ตรวจสอบความเป็นส่วนตัว (Privacy Settings) ตั้งค่าให้เฉพาะ "เพื่อน" เห็นโพสต์และปิดการแชร์พิกัดที่ตั้งโดยไม่จำเป็น

- Google ตัวเองบ่อย ๆ ลองค้นหาชื่อตัวเองดูว่ามีข้อมูลอะไรหลุดออกมาบ้าง เพื่อขอลบหรือแก้ไข

- แยกบัญชีใช้งาน แยกอีเมลสำหรับทำงาน และอีเมลสำหรับสมัครแอปฯ ทั่วไป เพื่อลดความเชื่อมโยงของข้อมูล

๒.๕.๒ การมีปฏิสัมพันธ์และการสร้างความร่วมมือในโลกดิจิทัล (Digital Interaction and Collaboration) คือ ทักษะการใช้เครื่องมือออนไลน์เพื่อทำงานร่วมกับผู้อื่นได้อย่างมีประสิทธิภาพและสร้างสายสัมพันธ์ที่ดีในสังคมดิจิทัล มีประเด็นสำคัญดังนี้

๑) รูปแบบการปฏิสัมพันธ์ในยุคใหม่

- การสื่อสารแบบ Real-time (Synchronous): เช่น การประชุมผ่าน Zoom, Google Meet หรือการแชทโต้ตอบทันที เหมาะสำหรับงานที่ต้องการการตัดสินใจด่วน

- การสื่อสารแบบไม่พร้อมกัน (Asynchronous): เช่น การใช้อีเมล, การฝากข้อความใน Slack หรือ Notion ข้อดีคือช่วยให้ผู้รับมีเวลาไตร่ตรองก่อนตอบ และไม่ขัดจังหวะการทำงานเชิงลึก (Deep Work)

๒) การสร้างความร่วมมือด้วยเครื่องมือดิจิทัล (Digital Collaboration) เพื่อให้งานหรือโครงการเดินหน้าได้อย่างราบรื่น ต้องอาศัยทักษะและเครื่องมือเหล่านี้

- การจัดการเอกสารร่วมกัน: การใช้ Cloud-based tools เช่น Google Workspace หรือ Microsoft 365 ที่ทุกคนสามารถแก้ไขงานในไฟล์เดียวกันได้พร้อมกัน (Co-authoring)

- การบริหารโครงการ (Project Management): ใช้แอปพลิเคชันอย่าง Trello, Asana หรือ Jira เพื่อมอบหมายงาน ติดตามสถานะ และทำให้ทุกคนเห็นภาพรวมของเป้าหมายเดียวกัน

- การแชร์ทรัพยากร: การใช้ระบบจัดเก็บข้อมูลออนไลน์ (Cloud Storage) เพื่อให้เข้าถึงข้อมูลได้จากทุกที่ทุกเวลา

๓) มารยาทและหัวใจสำคัญของการร่วมมือกัน

- ความชัดเจนในการสื่อสาร: เนื่องจากไม่มีภาษากาย การใช้ถ้อยคำที่ชัดเจนตรงประเด็น และสรุปประเด็นสำคัญ (Action Items) หลังจบการสนทนาจึงจำเป็นมาก

- การเคารพเวลาและพื้นที่ส่วนตัว: การมีปฏิสัมพันธ์ที่ดีต้องรู้จักขอบเขต เช่น ไม่ส่งเรื่องงานในกลุ่มแชทส่วนตัวในช่วงเวลาพักผ่อน

- ความรับผิดชอบ (Accountability): ในโลกดิจิทัลที่ทำงานแบบ Remote หรือ Hybrid ความซื่อสัตย์และการส่งงานตามกำหนดเป็นสิ่งเดียวที่สร้าง "ความเชื่อใจ" (Trust) ระหว่างทีม

๔) การจัดการความขัดแย้งออนไลน์

- Empathy (ความเห็นอกเห็นใจ): เข้าใจว่าข้อความตัวอักษรอาจสื่อสารอารมณ์ได้ไม่ครบถ้วน หากเริ่มมีความขัดแย้ง ควรเปลี่ยนจากการแชทมาเป็นการโทรศัพท์ หรือวิดีโอคอลเพื่อปรับความเข้าใจ

- การให้ Feedback: เน้นการวิจารณ์ที่ตัวงาน (Constructive Feedback) มากกว่าตัวบุคคล และใช้ช่องทางสื่อสารที่เป็นส่วนตัวเมื่อต้องพูดเรื่องที่ละเอียดอ่อน

๒.๖ Digital Disruption การปรับตัวในยุคดิจิทัล

๒.๖.๑ Digital Disruption คือ สถานการณ์ที่เทคโนโลยีดิจิทัล (เช่น AI, Blockchain, ๕G, IoT) เข้ามาสร้างโมเดลธุรกิจใหม่ที่ "ดีกว่า เร็วกว่า หรือถูกกว่า" จนทำให้ธุรกิจรูปแบบเดิมที่ปรับตัวไม่ทันต้อง

ปิดตัวลง หรือสูญเสียส่วนแบ่งการตลาดอย่างรวดเร็ว (เช่น Streaming ดิสรัป ร้านเช่าหนัง หรือ แอปสั่งอาหาร ดิสรัป ร้านอาหารแบบเดิม)

๒.๖.๒ เทรนด์สำคัญที่ต้องเจอ

- Hyper-Personalization: ลูกค้าคาดหวังบริการที่รู้ใจรายบุคคล โดยใช้ AI วิเคราะห์ข้อมูลแบบ Real-time
- AI-First Strategy: ไม่ใช่แค่ใช้ AI เป็นตัวช่วย แต่ AI จะกลายเป็นหัวใจหลักในการทำงาน และตัดสินใจ
- The Rise of AI Agents: การมี AI ที่ทำงานแทนมนุษย์ได้เกือบสมบูรณ์ในงานเฉพาะทาง ทำให้แรงงานต้องยกระดับไปทำงานเชิงกลยุทธ์มากขึ้น

๒.๖.๓ แนวทางการปรับตัว (Digital Transformation) เพื่อให้รอดพ้นจากการถูกดิสรัป ต้องปรับเปลี่ยนดังนี้

๑) ด้านความคิด (Mindset)

- Agile Mindset: ปรับตัวเร็ว ล้มเร็ว ลุกเร็ว พร้อมเรียนรู้สิ่งใหม่ (Lifelong Learning)
- Data-Driven: เลิกใช้ความรู้สึกตัดสินใจ แต่ใช้ "ข้อมูล" เป็นหลัก

๒) ด้านทักษะ (Skillset):

- Upskilling & Reskilling: ฝึกทักษะที่ AI ทำแทนไม่ได้ เช่น การคิดเชิงสร้างสรรค์ (Creative Thinking), ความฉลาดทางอารมณ์ (EQ), และการแก้ปัญหาที่ซับซ้อน
- Digital Fluency: ไม่ใช่แค่ใช้แอปเป็น แต่ต้องเข้าใจเทคโนโลยีและรู้วิธีนำมาประยุกต์ใช้กับงาน

๓) ด้านองค์กร (Organization):

- Customer Centric: ยึดลูกค้าเป็นศูนย์กลาง ไม่ใช่ยึดตามสินค้าที่ตัวเองมี
- Hybrid Workforce: ออกแบบการทำงานที่ผสมผสานระหว่างมนุษย์และ AI อย่างลงตัว

๔) ข้อควรระวัง

- Security & Privacy: ยิ่งใช้ดิจิทัลมาก ความเสี่ยงเรื่องข้อมูลรั่วไหลยิ่งสูง ต้องมีระบบ Cybersecurity ที่แข็งแกร่ง
- Digital Divide: ระวังช่องว่างทางดิจิทัลที่อาจทำให้คนกลุ่มหนึ่งเข้าไม่ถึงโอกาส

๓. ประโยชน์ที่ได้รับ มีความรู้ความเข้าใจในการใช้อินเทอร์เน็ต รู้เท่าทัน และมีความมั่นคงปลอดภัย

๔. แนวทางในการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน นำความรู้ที่ได้ไปประยุกต์ใช้ในการทำงานหาข้อมูลจากอินเทอร์เน็ตให้ได้ข้อมูลที่ถูกต้อง และปลอดภัย

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา สนับสนุนให้บุคลากรภายในหน่วยงานฯ ได้เรียนรู้ และฝึกฝนใช้อินเทอร์เน็ตในการหาข้อมูลที่ถูกต้องและปลอดภัย

(นายธิปไตย ไตรโภค)
ผู้เข้ารับการพัฒนาความรู้

(นางสุพัตรา บุรีรัตน์)
ผู้อำนวยการสำนักงานพัฒนาที่ดินเขต ๘
รักษาการในตำแหน่งผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ภาคผนวก

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ธิปไตย ไตรโภค

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Digital Literacy : ความฉลาดทางดิจิทัล

(Digital Intelligence)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 2 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ธิปไตย ไตรโภค

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

AI for Everyone : ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 2 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล