

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and using digital technology)

1. จริยธรรมการใช้เทคโนโลยีสารสนเทศ

ความหมายของ จริยธรรม (ethics) คือ หลักศีลธรรมที่กำหนดขึ้นเป็นแนวทางปฏิบัติหรือควบคุมระบบคอมพิวเตอร์และสารสนเทศ เป็นหลักของความถูกต้องที่ตกลงร่วมกันเพื่อเป็นแนวปฏิบัติในสังคม

จริยธรรมในการใช้งานคอมพิวเตอร์ 4 ประเด็น (PAPA)

- ความเป็นส่วนตัว (Privacy) ประกอบด้วย สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยแก่ผู้อื่น การละเมิดความเป็นส่วนตัว

- ความถูกต้อง (Accuracy) ประกอบด้วย การบันทึกข้อมูล มีผู้รับผิดชอบ การตรวจสอบ และมีความทันสมัย

- ความเป็นเจ้าของ (Property) ประกอบด้วย กรรมสิทธิ์ในการถือครอง ได้รับความคุ้มครองสิทธิภายใต้กฎหมาย และสิทธิความเป็นเจ้าของ

- การเข้าถึงข้อมูล (Data accessibility) ประกอบด้วย การกำหนดสิทธิตามระดับผู้ใช้งาน การป้องกันบุคคลภายนอก มีระบบรักษาความปลอดภัย

พ.ร.บ. ลิขสิทธิ์ มีหลัก 3 ประการของการไม่ละเมิดกฎหมายลิขสิทธิ์ คือ ขออนุญาต ให้เครดิต และห้ามดัดแปลง

ประเภททรัพย์สินทางปัญญา โดยทั่วไป เราสามารถแบ่งทรัพย์สินทางปัญญาออกเป็น 2 ประเภทใหญ่ๆ ตามลักษณะของความคิด ได้แก่

1. ทรัพย์สินทางอุตสาหกรรม ความคิดสร้างสรรค์ที่เกี่ยวข้องกับการผลิต การประกอบการ หรือการค้าขาย สิทธิบัตรการประดิษฐ์ สิทธิบัตรการออกแบบผลิตภัณฑ์ เครื่องหมายการค้า ความลับทางการค้า สิ่งบ่งชี้ทางภูมิศาสตร์ แบบผังภูมิของวงจรรวม และพันธุ์พืชใหม่

2. ลิขสิทธิ์ ความคิดสร้างสรรค์ทางวรรณกรรม ศิลปะ และบันเทิง งานวรรณกรรม (รวมโปรแกรมคอมพิวเตอร์) นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ ฯลฯ

รายละเอียดของทรัพย์สินทางปัญญาแต่ละประเภท

1. สิทธิบัตรการประดิษฐ์

คุ้มครองอะไร คิดค้นหรือค้นพบสูตร กระบวนการ หรือเครื่องจักร ที่เป็นสิ่งใหม่ มีขั้นการประดิษฐ์ที่สูงขึ้น และสามารถใช้ประโยชน์ทางอุตสาหกรรมได้

ตัวอย่าง ยารักษาโรคชนิดใหม่, เครื่องยนต์ที่ประหยัดพลังงานมากขึ้น

ระยะเวลาคุ้มครอง 20 ปี (ต้องยื่นขอรับสิทธิบัตร)

2. สิทธิบัตรการออกแบบผลิตภัณฑ์ (หรือ อนุสิทธิบัตรการออกแบบผลิตภัณฑ์)

คุ้มครองอะไร รูปร่าง ลวดลาย หรือสีสันทของผลิตภัณฑ์ที่แตกต่างไปจากเดิม และไม่ซ้ำกับที่มีอยู่

ตัวอย่าง การออกแบบรูปร่างของขวดน้ำหอม, ลวดลายบนพื้นรองเท้า

ระยะเวลาคุ้มครอง 10 ปี (ต้องยื่นขอรับสิทธิบัตร/อนุสิทธิบัตร)

3. เครื่องหมายการค้า

คุ้มครองอะไร สัญลักษณ์ ตรา เครื่องหมาย คำ ข้อความ หรือชื่อ ที่ใช้หรือจะใช้เป็นที่หมายถึงหรือเกี่ยวข้องกับสินค้าหรือบริการ เพื่อแสดงว่าสินค้าหรือบริการนั้นแตกต่างจากของรายอื่น

ตัวอย่าง โลโก้เครื่องหมายนกของ Nike, คำว่า "Starbucks", สีม่วงของช็อกโกแลต Cadbury

ระยะเวลาคุ้มครอง 10 ปี ต่ออายุได้เรื่อย ๆ (ต้องยื่นขอจดทะเบียน)

4. ความลับทางการค้า

คุ้มครองอะไร ข้อมูลทางการค้าที่ยังไม่เป็นที่รู้จักโดยทั่วไป มีมูลค่าในเชิงพาณิชย์ และเจ้าของได้ใช้มาตรการที่เหมาะสมในการรักษาความลับนั้น

ตัวอย่าง สูตรลับของโคคา-โคลา, รายชื่อลูกค้า, ซอสสูตรพิเศษของร้านอาหาร

ระยะเวลาคุ้มครอง ไม่มีกำหนด (ทราบเท่าที่ยังเก็บเป็นความลับได้)

5. สิ่งบ่งชี้ทางภูมิศาสตร์

คุ้มครองอะไร สินค้าที่มาจากแหล่งภูมิศาสตร์นั้น ๆ และมีคุณภาพ
ชื่อเสียง หรือลักษณะเฉพาะที่เกิดจากแหล่งดังกล่าว
ตัวอย่าง ข้าวหอมมะลิไทย, ชาเขียวอูจิ, ไวน์บอร์กโดซ์
ระยะเวลาคุ้มครอง ไม่มีกำหนด (ต้องขึ้นทะเบียน)

6. แบบผังภูมิของวงจรรวม

คุ้มครองอะไร การออกแบบวงจรไฟฟ้าในชิปหรือเซมิคอนดักเตอร์
(การจัดวางและเชื่อมต่อของทรานซิสเตอร์)

ระยะเวลาคุ้มครอง สูงสุด 10

ปี นับแต่วันที่สร้างสรรค์หรือนำออกเผยแพร่

7. พันธุ์พืชใหม่

คุ้มครองอะไร พืชที่ได้รับการปรับปรุงหรือพัฒนาให้มีลักษณะใหม่
แตกต่างไปจากพันธุ์เดิมที่มีอยู่ และมีความสม่ำเสมอคงตัว

ระยะเวลาคุ้มครอง 12-27 ปี ขึ้นอยู่กับชนิดของพืช

8. ลิขสิทธิ์

(รายละเอียดตามที่ได้กล่าวไปแล้วข้าง

ต้น) คุ้มครองงานสร้างสรรค์ทางวรรณกรรม ศิลปะ และบันเทิง เกิดขึ้น
ทันทีที่มีการสร้างสรรค์ โดยไม่ต้องจดทะเบียน

2. การเข้าถึงสื่อดิจิทัล

ในการจะเข้าถึงสื่อดิจิทัลได้อย่างสมบูรณ์ จำเป็นต้องมีองค์ประกอบ
3 ส่วนทำงานร่วมกัน

1. โครงสร้างพื้นฐาน (Physical Infrastructure) ที่ใช้ส่งข้อมูล
ได้แก่ สายเคเบิลใต้อะไหล่, เสาสัญญาณโทรศัพท์, ดาวเทียม และระบบ
เครือข่ายต่างๆ

2. อุปกรณ์ (Device) ที่เราใช้เดินบนถนนสายนั้น เพื่อดึงข้อมูลมา
แสดงผล

3. ซอฟต์แวร์และแพลตฟอร์ม (Software & Platform) ที่ทำให้
อุปกรณ์และเครือข่ายสื่อสารกันรู้เรื่อง รวมถึงแอปพลิเคชันที่เราใช้ เช่น
เบราว์เซอร์ (Chrome, Safari), โซเชียลมีเดีย (Facebook, TikTok), หรือ
Search Engine (Google, Bing)

อุปกรณ์ (Devices)

วิวัฒนาการของอุปกรณ์จากยุคบุกเบิกที่เป็นคอมพิวเตอร์ตั้งโต๊ะ เครื่องใหญ่ ปัจจุบันเราเห็นความหลากหลายมากขึ้น

- คอมพิวเตอร์ตั้งโต๊ะ (Desktop PC) เหมาะกับงานที่ต้องการพลังประมวลผลสูงและหน้าจอใหญ่
- โน้ตบุ๊ก (Notebook/Laptop) จุดสมดุลระหว่างประสิทธิภาพและการพกพา
- สมาร์ทโฟน (Smartphone) อุปกรณ์หลักแห่งยุค สำหรับการเข้าถึงสื่อทุกที่ทุกเวลา เพราะพกพาง่ายที่สุด
- แท็บเล็ต (Tablet) เหมาะกับการบริโภคสื่อ (ดูหนัง, อ่านหนังสือ) ที่ต้องการหน้าจอใหญ่กว่ามือถือ
- อุปกรณ์ IoT (Internet of Things) เช่น Smart TV, ลำโพงอัจฉริยะ (Google Home, Amazon Echo) ที่เชื่อมต่อเน็ตได้ในตัว

การค้นหาข้อมูล (Information Retrieval/Searching)

เครื่องมือที่ใช้ค้นหา (Search Engines) ที่นิยมใช้ในปัจจุบัน ได้แก่

- Google Search เครื่องมือค้นหาหลักของโลก ค้นหาได้ทั้งเว็บไซต์ รูปภาพ ข่าวสาร
- Search inside Platforms การค้นหาภายในแพลตฟอร์มนั้นๆ เช่น ค้นหาใน YouTube, ค้นหาใน TikTok, ค้นหาใน Pantip, หรือค้นหาสินค้าใน Shopee/Lazada

เทคนิคการค้นหาให้ตรงจุด (Search Tips)

- ใช้คำสำคัญ (Keywords) ยิ่งเฉพาะเจาะจงมากเท่าไร ผลลัพธ์ยิ่งตรงใจ เช่น แทนที่จะพิมพ์ "วิธีทำอาหาร" ให้พิมพ์ "วิธีทำผัดไทยกุ้งสด สูตรเส้นเหนียวนุ่ม"
- การใช้เครื่องหมายคำพูด (" ") เพื่อค้นหาข้อความที่เรียงกันเป๊ะๆ เช่น ค้นหาคำว่า "ประวัติศาสตร์อินเทอร์เน็ตในประเทศไทย"
- การใช้เครื่องหมายลบ (-) เพื่อไม่ให้รวมคำที่ไม่ต้องการ เช่น ค้นหา "เสื้อ" - "ฟุตบอล" (ถ้าต้องการหาเสื้อสัตว์ ไม่ใช่ทีมฟุตบอล)
- การใช้ตัวดำเนินการ (Operators) เฉพาะของ Google

- o site: ค้นหาภายในเว็บไซต์ใดเว็บไซต์หนึ่ง เช่น site:bbc.com climate change
- o filetype: ค้นหาไฟล์นามสกุลต่างๆ เช่น filetype:pdf รัฐธรรมนูญ 2560
- o related: หาเว็บไซต์ที่คล้ายกัน เช่น related:cnn.com

ทักษะการประเมินข้อมูล

การค้นหาเจอไม่ใช่จุดสิ้นสุด แต่ต้องรู้จักตั้งคำถามกับสิ่งที่เจอถึงความน่าเชื่อถือของข้อมูล ได้แก่

- ใครเป็นคนเขียน/เผยแพร่
- วันที่เผยแพร่ และการอัปเดตข้อมูล
- วัตถุประสงค์ของการให้ข้อมูล เช่นเพื่อขายของ โฆษณาชวนเชื่อ ให้ความรู้ หรือบันเทิง
- มีแหล่งอ้างอิงอื่นที่ยืนยันได้หรือไม่

3. ความเข้าใจและการสื่อสารยุคดิจิทัล

การเล่น social Network ให้ปลอดภัย

- คิดให้รอบ ก่อนโพสต์ โดยเฉพาะข้อมูลที่สุ่มเสี่ยงที่อาจจะเป็นภัยแก่ตนเอง
- ระมัดระวัง ในการคลิกลิงค์ที่มาจากการแชร์
- พิมพ์ URL โดยตรง ป้องกันการหลอกเอาข้อมูลของเรา
- รอบคอบ ก่อนตอบรับเป็นเพื่อนควรคัดกรองด้วยการดูโปรไฟล์ก่อนทุกครั้ง
- ตั้งค่าความเป็นส่วนตัว หลีกเลี่ยงการให้ข้อมูลส่วนตัวในที่สาธารณะ
- ไม่แสดงข้อมูลความเป็นส่วนตัวที่เป็นความลับ เช่นเลขที่บัตรประชาชน บัตรเครดิต
- เปิดใช้งาน Do Not track ป้องกันการติดตามและการเก็บข้อมูลจากผู้ไม่หวังดี

- ใช้วิจารณญาณในการรับข่าวสาร ต้องไม่ปักใจเชื่อทันที
- ควบคุมการใช้งานของบุตรหลาน
- ตระหนักว่าสังคมเสรีทุกคนมีสิทธิแสดงความคิดเห็นแต่ต้องอยู่ภายใต้กฎหมาย

4. ความปลอดภัยยุคดิจิทัล

Digital

Footprint หรือ "ร่องรอยทางดิจิทัล" คือ ประวัติการใช้งานออนไลน์ทั้งหมดของเราที่ถูกบันทึกไว้บนโลกอินเทอร์เน็ต เหมือนกับรอยเท้าที่เราทิ้งไว้บนหาดทราย แต่รอยนี้จะอยู่ไปตลอดกาลและลบได้ยากมาก

ภัยคุกคามที่พบบ่อยในยุคดิจิทัล

**ประเภทภัย
คุกคาม**

คำอธิบาย

ตัวอย่าง

**ฟิชซิง
(Phishing)**

การหลอกลวงให้เราหลงเชื่อ โดยส่งข้อความหรือลิงก์ปลอมที่แอบอ้างเป็นคนหรือองค์กรที่เราไว้วางใจ เพื่อให้เรากรอกข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลบัตรเครดิต

อีเมลแจ้งว่าธนาคารกำลังอัปเดตระบบ ให้กดลิงก์เพื่อยืนยันตัวตน ซึ่งลิงก์นั้นจะพาไปหน้าเว็บปลอมที่เหมือนจริงมาก

**มัลแวร์
(Malware)**

ซอฟต์แวร์อันตรายที่ถูกออกแบบมาเพื่อแทรกซึมหรือสร้างความเสียหายให้กับอุปกรณ์ของเรา

- ไวรัส แทรกตัวเองไปยังไฟล์อื่น ๆ
- แรนซัมแวร์ เข้ารหัสไฟล์ในเครื่องเรา แล้วเรียกค่าไถ่ให้จ่ายเงินเพื่อปลดล็อก

ประเภทภัยคุกคาม

คำอธิบาย

ตัวอย่าง

การโจรกรรมข้อมูล/ตัวตน

การที่มิจฉาชีพขโมยข้อมูลส่วนตัวของเราไปใช้แอบอ้างทำสิ่งผิดกฎหมาย หรือก่อหนี้

แฮกเกอร์เจาะระบบเว็บไซต์แล้วได้ข้อมูลชื่อ-นามสกุล บัตรประชาชน เบอร์โทรศัพท์ของเราไปเปิดบัญชีธนาคารหรือกู้เงินออนไลน์

การดักฟังข้อมูล (Man-in-the-Middle)

การแอบดักข้อมูลระหว่างที่เรากำลังส่งข้อมูลไปยังเว็บไซต์ โดยเฉพาะเวลาใช้ Wi-Fi สาธารณะที่ไม่ปลอดภัย

ขณะที่นั่งทำงานในร้านกาแฟและต่อ Wi-Fi ฟรี มีแฮกเกอร์ในเครือข่ายเดียวกันดักจับรหัสผ่านที่เรากำลังพิมพ์ส่งไปยังอีเมล

วิศวกรรมสังคม (Social Engineering)

การหลอกลวงโดยใช้จิตวิทยา ชักจูงให้เรายอมทำอะไรบางอย่างหรือเปิดเผยข้อมูลเอง โดยไม่ต้องใช้เทคโนโลยีขั้นสูง

มิจฉาชีพโทรศัพท์มาอ้างว่าเป็นเจ้าหน้าที่บริษัทไปรษณีย์ มีพัสดุตกค้างแล้วขอให้เราแจ้งข้อมูลส่วนตัวเพื่อยืนยันตัวตน

แนวทางการป้องกันตนเอง

1. การจัดการรหัสผ่าน (Password Hygiene)
 - ตั้งรหัสผ่านที่คาดเดายาก ไม่ใช่วันเกิด ชื่อสัตว์เลี้ยง หรือ 1234 ควรผสมตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ
 - ไม่ใช้รหัสผ่านซ้ำกัน: หากรหัสผ่านของเว็บหนึ่งรั่วไหล มิจฉาชีพจะลองเอาไปใช้กับเว็บอื่น ๆ ของเราด้วย (Credential Stuffing)

- ใช้ตัวจัดการรหัสผ่าน (Password Manager) โปรแกรมช่วยจำรหัสผ่านที่ซับซ้อน เราต้องจำแค่รหัสผ่านหลักเพียงอันเดียว
- เปิดการยืนยันตัวตนสองขั้นตอน (2FA - Two-Factor Authentication): นี้คือเกราะป้องกันที่ดีที่สุด นอกจากการใส่รหัสผ่านแล้ว ต้องมีอีกขั้นตอนยืนยัน เช่น รหัสจาก SMS, แอปฯ Google Authenticator, หรือลายนิ้วมือ ถึงแม้รหัสผ่านจะรั่ว แฮกเกอร์ก็เข้าไม่ได้ถ้าไม่มีขั้นตอนที่สอง

2. การใช้งานอุปกรณ์และเครือข่าย

- อัปเดตซอฟต์แวร์เสมอ การอัปเดตระบบปฏิบัติการ (iOS, Android, Windows) และแอปฯ ต่าง ๆ ไม่ใช่แค่เพิ่มฟีเจอร์ แต่เป็นการ อัปเดตช่องโหว่ด้านความปลอดภัย ที่เพิ่งถูกค้นพบ
- ระวัง Wi-Fi สาธารณะ หลีกเลี่ยงการทำธุรกรรมทางการเงิน (เข้าแอปธนาคาร, ซื้อของออนไลน์) ขณะใช้ Wi-Fi ฟรีที่ไม่มีการเข้ารหัส หากจำเป็นต้องใช้ VPN (Virtual Private Network) เพื่อเข้ารหัสข้อมูล
- ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus/Anti-malware) โดยเฉพาะบนคอมพิวเตอร์ Windows ช่วยสกัดกั้นภัยคุกคามเบื้องต้นได้

การรู้เท่าทันกลโกง (Human Firewall)

- อย่าเพิ่งเชื่อ อย่าเพิ่งคลิก ก่อนคลิกลิงก์ใด ๆ ให้เอาเมาส์ชี้ดู (โดยไม่คลิก) ว่าลิงก์ปลายทางคืออะไร ตรงกับที่แจ้งหรือไม่
- เช็กก่อนแชร์ข้อมูล ไม่มีหน่วยงานใด (โดยเฉพาะธนาคารหรือตำรวจ) ขอให้เรากรอกรหัสผ่านหรือโอนเงินผ่านทางโทรศัพท์หรือลิงก์ที่ส่งมาให้
- ตั้งสติก่อนโอนเงิน ถ้ามีคน (แม้แต่เพื่อนหรือญาติ) ทักมาขอให้โอนเงินด่วน ควรโทรศัพท์ไปหาจริงๆ เพื่อยืนยันตัวตนก่อน เพราะบัญชีโซเชียลอาจถูกแฮ็กได้

นางสาววนิดา งามเงิน
นักวิชาการเกษตรชำนาญการพิเศษ
กลุ่มวิจัยและพัฒนาการใช้ประโยชน์หญ้าแฝกในการจัดการดิน

สรุปการอบรม ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and Using Digital Technology Effectively)

การอบรมเรื่อง “ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ” มีวัตถุประสงค์เพื่อพัฒนาความรู้ ทักษะ และทัศนคติที่เหมาะสมในการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์สูงสุดต่อการทำงาน การเรียนรู้ และการดำเนินชีวิตประจำวัน โดยเน้นทั้งด้านประสิทธิภาพ ความปลอดภัย และจริยธรรมในการใช้งาน

1. ความหมายและความสำคัญของเทคโนโลยีดิจิทัล

เทคโนโลยีดิจิทัลหมายถึง เครื่องมือ ระบบ หรือแพลตฟอร์มที่ใช้ข้อมูลในรูปแบบดิจิทัล เช่น คอมพิวเตอร์ อินเทอร์เน็ต ระบบคลาวด์ แอปพลิเคชัน และสื่อสังคมออนไลน์ ซึ่งมีบทบาทสำคัญในการสื่อสาร การบริหารจัดการข้อมูล การวิเคราะห์ข้อมูล และการตัดสินใจเชิงนโยบาย การเข้าใจหลักการการทำงานพื้นฐานจะช่วยให้สามารถเลือกใช้เทคโนโลยีได้เหมาะสมกับบริบทงาน

2. การใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพการทำงาน

ผู้เข้าอบรมได้เรียนรู้การใช้เครื่องมือดิจิทัลเพื่อเพิ่มผลิตภาพ (Productivity) เช่นการจัดเก็บและแชร์เอกสารผ่านระบบคลาวด์ การใช้โปรแกรมตารางคำนวณและฐานข้อมูลในการวิเคราะห์ข้อมูล การใช้แพลตฟอร์มประชุมออนไลน์เพื่อการสื่อสารแบบประสานเวลา (Synchronous) การจัดการงานผ่านระบบออนไลน์และแอปพลิเคชันบริหารโครงการ การเลือกใช้เครื่องมือที่เหมาะสมช่วยลดขั้นตอนการทำงาน ลดความซ้ำซ้อน และเพิ่มความรวดเร็วในการดำเนินงาน

3. ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

การใช้เทคโนโลยีอย่างมีประสิทธิภาพต้องควบคู่กับความปลอดภัย ผู้เข้าอบรมได้ตระหนักถึงความเสี่ยง เช่น มัลแวร์ ฟิชซิง และการโจมตีทางไซเบอร์ พร้อมทั้งแนวทางป้องกัน ได้แก่ การตั้งรหัสผ่านที่รัดกุม การใช้ระบบยืนยันตัวตนหลายชั้น (Multi-factor Authentication) การหลีกเลี่ยงการเชื่อมต่อเครือข่ายที่ไม่ปลอดภัย การสำรองข้อมูลอย่างสม่ำเสมอ

4. จริยธรรมและความรับผิดชอบทางดิจิทัล

การใช้งานดิจิทัลต้องคำนึงถึงความเป็นส่วนตัว (Privacy) ลิขสิทธิ์ (Copyright) และความถูกต้องของข้อมูล (Information Integrity) ผู้เข้าอบรมได้เรียนรู้การเคารพสิทธิผู้อื่น ไม่เผยแพร่ข้อมูลเท็จ และใช้สื่อออนไลน์อย่างสร้างสรรค์ รวมถึงการอ้างอิงแหล่งที่มาของข้อมูลอย่างถูกต้อง

5. การรู้เท่าทันข้อมูล (Digital Literacy)

เนื้อหาการอบรมเน้นการวิเคราะห์และประเมินความน่าเชื่อถือของข้อมูล การแยกแยะข้อเท็จจริงกับความคิดเห็น และการใช้ข้อมูลประกอบการตัดสินใจอย่างมีเหตุผล ซึ่งเป็นทักษะสำคัญในยุคข้อมูลข่าวสารจำนวนมาก (Big Data)

สรุปภาพรวม

การอบรมครั้งนี้ช่วยเสริมสร้างความเข้าใจเชิงระบบเกี่ยวกับเทคโนโลยีดิจิทัล ทั้งด้านการใช้งานอย่างมีประสิทธิภาพ ความปลอดภัย และความรับผิดชอบต่อสังคม ผู้เข้าอบรมสามารถนำความรู้ไปประยุกต์ใช้ในการทำงาน เพื่อเพิ่มประสิทธิภาพองค์กร ลดความเสี่ยง และสนับสนุนการพัฒนางานองค์กรสู่การเป็นหน่วยงานดิจิทัลอย่างยั่งยืน

กล่าวโดยสรุป เทคโนโลยีดิจิทัลไม่ใช่เพียงเครื่องมือ แต่เป็นกลไกสำคัญในการขับเคลื่อนการพัฒนา หากมีความเข้าใจและใช้อย่างถูกต้อง ย่อมก่อให้เกิดประโยชน์สูงสุดทั้งต่อบุคคล องค์กร และสังคมโดยรวม