ประกาศการท่าเรือแห่งประเทศไทย
เรื่อง นโยบายการกำกับดูแลการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล

การท่าเรือแห่งประเทศไทย มุ่งมั่นผลักดันให้มีการนำเทคโนโลยีดิจิทัลที่เหมาะสมมาใช้ในการปฏิบัติงานภายในองค์กร และอำนวยความสะดวกในการให้บริการแก่ผู้มีส่วนได้ส่วนเสียทุกกลุ่ม ซึ่งในปัจจุบันเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) ได้เข้ามามีบทบาทในกิจกรรมด้านต่าง ๆ ทั้งในระบบงานด้านการบริหารจัดการ ระบบงานด้านปฏิบัติการ การประมวลผลข้อมูล การจัดทำข้อมูล ดังนั้น เพื่อให้การพัฒนาและการประยุกต์ใช้ AI มีประสิทธิภาพ น่าเชื่อถือ มั่นคงปลอดภัย ก่อให้เกิดประโยชน์กับสังคมและสิ่งแวดล้อม ด้วยความโปร่งใส ครอบคลุมและเป็นธรรม สอดคล้องตามกฎหมาย จริยธรรม และสิทธิมนุษยชน จึงได้กำหนดนโยบายการกำกับดูแลการประยุกต์ใช้ AI อย่างมีธรรมาภิบาลของการท่าเรือแห่งประเทศไทย ดังนี้

ข้อ ๑ กำหนดให้มีโครงสร้างการกำกับดูแลการประยุกต์ใช้ AI พร้อมกำหนดบทบาทหน้าที่เพื่อกำกับดูแลการพัฒนาและประยุกต์ใช้ AI ให้สอดคล้องกับเป้าหมายขององค์กรอย่างมีธรรมาภิบาล จริยธรรม มั่นคงปลอดภัย สอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ข้อ ๒ สนับสนุนให้มีการพัฒนาและประยุกต์ใช้ AI เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานและยกระดับการให้บริการของ กทท.

ข้อ ๓ ส่งเสริมบุคลากรให้มีความตระหนักรู้ต่อความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability) มีความเข้าใจเทคโนโลยี AI รวมทั้งข้อจำกัดและความเสี่ยงของเทคโนโลยีนี้ เพื่อให้สามารถนำไปประยุกต์ใช้ให้เกิดประโยชน์อย่างเหมาะสม

ข้อ ๔ บริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการพัฒนาและประยุกต์ใช้ AI พร้อมจัดทำแนวทางจัดการความเสี่ยงที่อาจเกิดขึ้นอย่างเหมาะสม

ข้อ ๕ จัดให้มีช่องทางการสื่อสาร รับฟังข้อคิดเห็น ประเด็นปัญหาจากการปฏิบัติงานและการให้บริการ พร้อมทั้งจัดให้มีมาตรการแก้ไขปัญหา และรับมือกับเหตุการณ์ผิดปกติได้ทันท่วงที

ข้อ ๖ ติดตาม เฝ้าระวังผลกระทบเกี่ยวกับการพัฒนาและการประยุกต์ใช้ AI อย่างสม่ำเสมอ

ข้อ ๗ ประเมินผลการประยุกต์ใช้ AI พร้อมนำผลลัพธ์มาพิจารณากำหนดแนวทางการดำเนินงานในอนาคต เพื่อการพัฒนาปรับปรุงอย่างต่อเนื่อง

ข้อ ๘ ทบทวนนโยบายและแนวปฏิบัติการกำกับดูแลการประยุกต์ใช้ AI อย่างมีธรรมาภิบาลของการท่าเรือฯ อย่างน้อยปีละหนึ่งครั้ง หรือมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

ข้อ ๙ ให้ถือปฏิบัติตามแนวปฏิบัติการกำกับดูแลการประยุกต์ใช้ AI อย่างมีธรรมาภิบาลของการท่าเรือฯ ที่แนบท้ายนโยบายฉบับนี้

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ เมษายน พ.ศ. ๒๕๖๙

ว่าที่ร้อยตรี
(รัฐกร เขียวไพศาล)
รองผู้อำนวยการการท่าเรือฯ สายบริหารการเงินและกลยุทธ์องค์กร
รักษาการแทน ผู้อำนวยการการท่าเรือแห่งประเทศไทย

แนวปฏิบัติการกำกับดูแลการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล

(AI Governance Guideline)

การท่าเรือแห่งประเทศไทย

ฝ่ายเทคโนโลยีสารสนเทศ

สารบัญ

แนวปฏิบัติการกำกับดูแลการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล
การท่าเรือแห่งประเทศไทย

บทนำ

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นเทคโนโลยีที่ถูกใช้อย่างแพร่หลายและกำลังได้รับความนิยมอย่างมาก เนื่องด้วยศักยภาพของปัญญาประดิษฐ์ที่สามารถประยุกต์ใช้กับหลากหลายวงการ ขณะเดียวกันหากผู้ที่เกี่ยวข้อง วิจัย ออกแบบ พัฒนา หรือใช้ในทางที่ไม่ถูกต้อง ละเมิดกฎหมายหรือจริยธรรมพื้นฐาน ทั้งที่ตั้งใจหรือรู้เท่าไม่ถึงการณ์ก็ตาม พลังอำนาจของปัญญาประดิษฐ์ รวมถึงวิทยาศาสตร์ข้อมูล (Data Science) ที่ใช้ปัญญาประดิษฐ์ เช่น การเรียนรู้ด้วยเครื่อง (Machine Learning) การเรียนรู้เชิงลึก (Deep Learning) หรือใช้อัลกอริทึมที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Algorithm) ที่พัฒนาอย่างรวดเร็วนี้ ก็อาจนำมาซึ่งภัยร้ายแรงต่อมนุษย์ สังคม และสิ่งแวดล้อมได้เช่นกัน หากไม่มีการกำกับดูแลอย่างเหมาะสม

แนวปฏิบัติการกำกับการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล ของการท่าเรือแห่งประเทศไทย (กทท.) ฉบับนี้จัดทำขึ้นเพื่อใช้เป็นแนวทางสำหรับการดำเนินงานของ กทท. และให้ผู้รับบริการได้ทราบถึงสิทธิและตระหนักรู้ถึงความเสี่ยงของการใช้ปัญญาประดิษฐ์ และเป็นแนวทางในการส่งเสริม สนับสนุน รวมถึงกำกับดูแลเทคโนโลยีปัญญาประดิษฐ์ เพื่อทำให้ปัญญาประดิษฐ์มีความน่าเชื่อถือ มั่นคงปลอดภัย ได้รับการพัฒนาและใช้งาน ก่อให้เกิดประโยชน์กับสังคมและสิ่งแวดล้อม ด้วยความโปร่งใส ครอบคลุมและเป็นธรรม สอดคล้องตามกฎหมาย จริยธรรมและสิทธิมนุษยชน

วัตถุประสงค์

1) เพื่อให้การพัฒนาและการประยุกต์ใช้ AI มีประสิทธิภาพ น่าเชื่อถือ มั่นคงปลอดภัย ก่อให้เกิดประโยชน์กับสังคมและสิ่งแวดล้อม ครอบคลุมและเป็นธรรม สอดคล้องตามกฎหมาย จริยธรรมและสิทธิมนุษยชน สามารถบรรลุตามเป้าหมายขององค์กรอย่างมีความรับผิดชอบ ซึ่งจะนำไปสู่ความเชื่อมั่นและการยอมรับจากผู้ที่เกี่ยวข้องในทุกภาคส่วน
2) เพื่อเป็นแนวทางการพัฒนาและการประยุกต์ใช้ AI อย่างเหมาะสมสำหรับพนักงาน ลูกจ้าง และผู้ปฏิบัติงานที่เกี่ยวข้อง
3) เพื่อส่งเสริมสร้างความตระหนักรู้และความเข้าใจเกี่ยวกับการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ สามารถใช้งานได้อย่างถูกต้องเหมาะสมและเป็นไปตามแนวทางที่องค์กรกำหนดไว้

ขอบเขต

เอกสารนี้จัดทำโดยมีวัตถุประสงค์เพื่อนำเสนอแนวทางการกำกับดูแลการประยุกต์ใช้ AI ในภาพรวม โดยไม่มีการระบุเฉพาะเจาะจงประเภทของเทคโนโลยี ดังนั้นจึงควรพิจารณาถึงความเหมาะสมกับบริบทของการนำ AI ไปประยุกต์ใช้ เทคโนโลยีที่ใช้ การเปลี่ยนแปลงของเทคโนโลยีในอนาคต ความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง รวมถึงความเสี่ยงที่เกี่ยวข้อกับบริบทของการนำ AI ไปประยุกต์ใช้ เช่น ภัยคุกคามทางไซเบอร์ เป็นต้น

บทสรุปผู้บริหาร

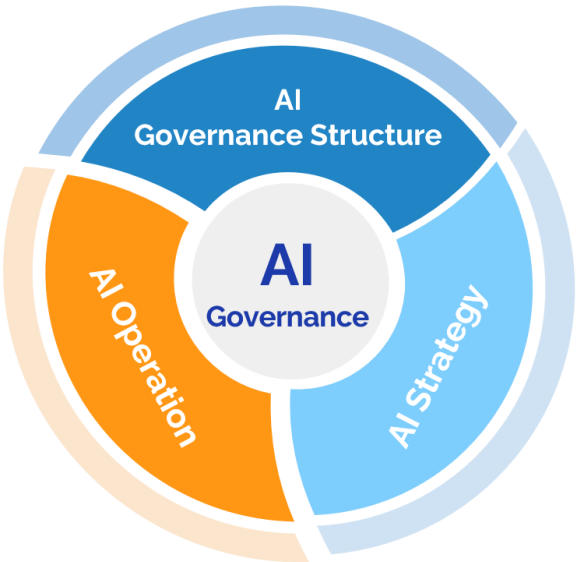
เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์มากขึ้น จึงทำให้ทั่วโลกเกิดความกังวลถึงผลกระทบที่อาจเกิดขึ้นกับมนุษย์ในด้านต่าง ๆ อาทิ ด้านจริยธรรม ด้านความเป็นธรรม ด้านความเป็นส่วนตัว และด้านความปลอดภัย รวมถึงความรับผิดชอบจากผลกระทบอันเกิดจากการนำ AI มาช่วยเหลือหรือตัดสินใจแทนมนุษย์ เป็นต้น

ด้วยเหตุนี้ **ธรรมาภิบาลในการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance) หรือหลักการในการกำกับดูแลการประยุกต์ใช้ AI ที่ดี**นั้น จึงเป็นเรื่องสำคัญที่องค์กรจำเป็นต้องดำเนินการตามบริบทขององค์กรอย่างเหมาะสม เพื่อให้การประยุกต์ใช้ AI สามารถบรรลุตามเป้าหมายที่องค์กรกำหนด และมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง (Responsible Use of AI) โดยคำนึงถึงหลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) ความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Laws and Regulations) รวมถึงการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI

AI Governance มีเป้าหมายเพื่อให้การประยุกต์ใช้ AI บรรลุตามเป้าหมายขององค์กร อย่างมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง

เอกสาร “**แนวปฏิบัติการกำกับการประยุกต์ใช้ AI อย่างมีธรรมาภิบาล**” นำเสนอแนวปฏิบัติสำหรับการกำกับดูแลการประยุกต์ใช้ AI พร้อมทั้งนำเสนอตัวอย่างแนวปฏิบัติทั้งจากภายในและต่างประเทศ รวมถึงแนวปฏิบัติตามมาตรฐานสากล เพื่อเป็นแนวทางให้การประยุกต์ใช้ AI ในองค์กรสามารถบรรลุตามเป้าหมายที่กำหนดอย่างมีความรับผิดชอบ ซึ่งจะนำไปสู่ความเชื่อมั่นและการยอมรับจากผู้ที่เกี่ยวข้องในทุกภาคส่วน

แนวทางในการกำกับดูแล ซึ่งประกอบด้วย 3 องค์ประกอบหลัก



1. **การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure)**

เป็นการนำเสนอแนวทางการกำหนดโครงสร้างการกำกับดูแลการประยุกต์ใช้ AI ขององค์กร โดยมีคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) ซึ่งมีหน้าที่ในการกำหนดกลยุทธ์และนโยบายที่เกี่ยวข้องเพื่อขับเคลื่อนการประยุกต์ใช้ AI ภายในองค์กร รวมถึงมีหน้าที่ในการเฝ้าติดตามและประเมินผลการประยุกต์ใช้ AI อย่างเหมาะสม นอกจากกำหนดคณะกรรมการเพื่อกำกับดูแลโดยภาพรวมแล้ว องค์กรยังจำเป็นต้องกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) ของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (Stakeholders) ตามโครงสร้างการกำกับดูแล พร้อมทั้งสนับสนุนทรัพยากรที่จำเป็น ส่งเสริมทักษะความรู้ รวมถึงสร้างความตระหนักรู้ (Awareness) ต่อความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability) ของแต่ละหน้าที่อีกด้วย

2. **การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)**

เป็นการมองหาโอกาสหรือประโยชน์ที่องค์กรจะได้รับจากการนำ AI มาประยุกต์ใช้ที่ตอบสนองเป้าหมายขององค์กร พร้อมทั้งวิเคราะห์เป้าหมายความสำเร็จจากการนำ AI มาประยุกต์ใช้ ความเป็นไปได้ในการดำเนินการ ความพร้อมขององค์กร และทรัพยากรที่จำเป็น เพื่อให้มั่นใจได้ว่าการประยุกต์ใช้ AI จะบรรลุตามเป้าหมายและประสบความสำเร็จตามที่กำหนด นอกจากนี้ในการกำหนดกลยุทธ์ยังจำเป็นต้องวิเคราะห์ถึงความเสี่ยงและผลกระทบจากการนำ AI มาประยุกต์ใช้ควบคู่ไปกับความสอดคล้องกับหลักการจริยธรรมปัญญาประดิษฐ์และความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง เพื่อแสดงให้เป็นถึงความมุ่งมั่นขององค์กรที่จะประยุกต์ใช้ AI อย่างมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง (Responsible Use of AI)

3. **การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)**

เป็นการอธิบายถึงแนวปฏิบัติตลอดวงจรชีวิตของ AI (AI Lifecycle) เพื่อให้มั่นใจได้ว่า AI ได้รับการออกแบบ พัฒนา และไปใช้งานได้อย่างสอดคล้องตามเป้าหมายขององค์กร รวมถึงสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง นอกจากนี้ ยังอธิบายถึงแนวปฏิบัติในการจัดเตรียมข้อมูล (Data Preparation) เพื่อให้ได้ข้อมูลที่มีคุณภาพและเหมาะสมสำหรับนำไปใช้สอนและทำงานร่วมกับ AI รวมถึงแนวปฏิบัติการรับมือกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น การเฝ้าติดตามและการประเมินผลการประยุกต์ใช้งาน AI เพื่อปรับปรุงการดำเนินงานให้มีประสิทธิภาพต่อไปในอนาคต

จากแนวทางในการกำกับดูแลทั้ง 3 องค์ประกอบหลักข้างต้น เป็นการนำเสนอแนวทางการกำกับดูแลการประยุกต์ใช้เทคโนโลยี AI อย่างมีธรรมาภิบาล โดยมี**คณะกรรมการกำกับดูแลการประยุกต์ใช้ AI ซึ่งมีหน้าที่หลักในการกำกับดูแลในภาพรวม ตั้งแต่การกำหนดกลยุทธ์และนโยบาย การควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้นไปจนถึงการกำกับดูแลการปฏิบัติงานตลอดวงจรชีวิตของ AI พร้อมทั้ง กำหนดหน้าที่และความรับผิดชอบของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องอย่างชัดเจน** เพื่อให้มั่นใจว่าการประยุกต์ใช้ AI ขององค์กร จะบรรลุตามเป้าหมายที่กำหนดและมีความรับผิดชอบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง ซึ่งจะทำให้เกิดความเชื่อมั่นและได้รับการยอมรับจากทุกภาคส่วน

นิยาม

องค์กร หมายถึง การท่าเรือแห่งประเทศไทย (กทท.)

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) หมายถึง เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ รวบรวมองค์ความรู้ในหลายสาขาวิชาโดยเฉพาะอย่างยิ่งทางด้านวิทยาศาสตร์และวิศวกรรมศาสตร์มาพัฒนาให้เครื่องจักรหรือระบบคอมพิวเตอร์มีความชาญฉลาด สามารถคิด คำนวณ วิเคราะห์ เรียนรู้และตัดสินใจ โดยใช้เหตุผลได้เสมือนสมองของมนุษย์ และสามารถเรียนรู้ พัฒนาและปรับปรุงกระบวนการทำงานเพื่อเพิ่มศักยภาพของปัญญาประดิษฐ์เองได้

Machine Learning (ML) หมายถึง เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถในการเรียนรู้หรือปรับปรุงประสิทธิภาพการทำงานของตน โดยใช้อัลกอริทึมในการวิเคราะห์ และเรียนรู้จากข้อมูลที่ได้รับจากการสอนหรือสภาพแวดล้อม

Deep Learning (DL) หมายถึง Machine Learning ประเภทหนึ่งที่ประมวลผลผ่านโครงข่ายประสาทเทียม (Artificial Neural Network: ANN) จำนวนหลายชั้น (Layer) ที่ถูกสร้างขึ้นจากข้อมูลที่ได้รับการฝึกฝน เพื่อให้สามารถทำงานหรือสร้างผลลัพธ์ที่มีประสิทธิภาพดียิ่งขึ้น

Artificial Neural Network (ANN) หมายถึง โครงข่ายของเซลล์ประสาทเทียม (Artificial Neuron) ที่คล้ายกับการเชื่อมต่อเซลล์ประสาท (Neuron) ในสมองมนุษย์ โดยใน แต่ละเซลล์ประสาทเทียมนั้น มีหน้าที่ในการรับข้อมูลและนำไปประมวลผลเพื่อสร้างเป็นผลลัพธ์ จากนั้นจึงส่งต่อผลลัพธ์ไปยังเซลล์ประสาทเทียมในชั้น (Layer) ถัดไปเพื่อประมวลผลต่อ

โมเดลปัญญาประดิษฐ์ (AI Model) หมายถึง โปรแกรมที่ถูกสร้างขึ้นจากอัลกอริทึมและข้อมูลที่สอนโดยมนุษย์เพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เป็นประเภทหนึ่งของแมชชีนเลิร์นนิ่ง (Machine Learning) เท่านั้น ที่จำเป็นต้องมีการเรียนรู้จากข้อมูลที่สอนโดยมนุษย์

Generative AI หมายถึง เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถในการสร้างเนื้อหาใหม่ในหลากหลายรูปแบบ เช่น ข้อความ ภาพ วิดีโอ ซอร์สโค้ด หรือรูปแบบอื่น เป็นต้น ตามข้อความหรือคำสั่ง (Prompt) ที่มนุษย์เป็นผู้กำหนด

Prompt Engineering หมายถึง การสร้างและปรับแต่งข้อความหรือคำสั่ง เพื่อให้ Generative AI สร้างผลลัพธ์ (Output) ที่ดีที่สุดและตรงตามความต้องการ

Foundation Model หมายถึง โมเดล AI ประเภท Generative AI ที่ได้รับการฝึกฝนด้วยข้อมูลขนาดใหญ่ โดยมีวัตถุประสงค์เพื่อให้สามารถสร้างเนื้อหาใหม่ที่คล้ายคลึงกับข้อมูลที่ได้รับการฝึกฝน

Large Language Model (LLM) หมายถึง โมเดลภาษาขนาดใหญ่ที่รับข้อความหรือคำสั่ง (Input) ในรูปแบบภาษาและนำไปสร้างผลลัพธ์ (Output) ที่มีความสามารถในด้านภาษาที่หลากหลาย เช่น การสร้างข้อความใหม่ การแปลภาษา การสรุปความ การวิเคราะห์ข้อความ เป็นต้น

หลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) หมายถึง หลักการในการออกแบบและพัฒนาให้พฤติกรรมหรือผลลัพธ์จากการทำงานของ AI สอดคล้องตามหลักการจริยธรรมหรือหลักการอันดีที่พึงปฏิบัติตามบริบทที่ AI ถูกนำไปประยุกต์ใช้

หลักการในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ (Responsible AI) หมายถึง หลักการในการนำ AI มาประยุกต์ใช้เพื่อประโยชน์ของบุคคลที่เกี่ยวข้องกับองค์กร อย่างมีความรับผิดชอบต่อผลกระทบที่อาจเกิดขึ้นกับบุคคล องค์กร และสังคมโดยกว้าง เพื่อนำไปสู่การสร้างความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้องในทุกภาคส่วน

ผู้ออกแบบปัญญาประดิษฐ์ หมายถึง ผู้มีหน้าที่ศึกษาและวิเคราะห์ความต้องการของผู้ใช้งานปัญญาประดิษฐ์มาจัดทำแบบแผนในการสร้างปัญญาประดิษฐ์ เพื่อให้สามารถใช้งานได้จริงและตรงตามความต้องการของผู้ใช้งานปัญญาประดิษฐ์

ผู้พัฒนาปัญญาประดิษฐ์ หมายถึง ผู้มีหน้าที่พัฒนาปัญญาประดิษฐ์ตามแบบแผนที่ผู้ออกแบบปัญญาประดิษฐ์ออกแบบไว้ และทำการทดสอบใช้งานปัญญาประดิษฐ์เพื่อตรวจสอบว่าปัญญาประดิษฐ์สามารถใช้งานได้จริงและตรงตามความต้องการ

ผู้ใช้งานปัญญาประดิษฐ์ หมายถึง กลุ่มบุคคลผู้เป็นผู้รับบริการปัญญาประดิษฐ์ โดยมีหน้าที่ระบุปัญหา และความต้องการที่ต้องการให้ปัญญาประดิษฐ์ให้ความช่วยเหลือและแก้ไขปัญหาให้ โดยหมายความรวมถึงประชาชนทุกคนและกลุ่มคนส่วนน้อย เช่น ผู้ด้อยโอกาส ผู้พิการ และผู้ทุพพลภาพ

ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) หมายถึง ผู้ให้บริการที่นำเทคโนโลยี AI มาพัฒนาเป็นโซลูชั่นหรือซอฟต์แวร์ เพื่อให้บริการแก่บุคคลหรือองค์กรที่ต้องการนำเทคโนโลยี AI ไปประยุกต์หรือปรับใช้ตามวัตถุประสงค์ที่ต้องการ

หน่วยงานควบคุมดูแลการพัฒนาและใช้งานปัญญาประดิษฐ์ หมายถึง หน่วยงานภาครัฐ ผู้มีหน้าที่ควบคุม กำกับดูแล บุคคลและหน่วยงานที่เกี่ยวข้องกับการวิจัย ออกแบบ พัฒนา และใช้งานปัญญาประดิษฐ์ ให้สอดคล้องกับจริยธรรมปัญญาประดิษฐ์ในทุกขั้นตอนการทำงาน โดยมีการกำหนดอำนาจ หน้าที่ความรับผิดชอบ และบทลงโทษไว้อย่างชัดเจน

ความโปร่งใส (Transparency) หมายถึง การที่สามารถอธิบายเหตุการณ์ การกระทำ กระบวนการทำงาน และกิจกรรมต่าง ๆ ที่เกิดขึ้นย้อนหลังได้ทั้งหมด เพื่อให้หน่วยงานควบคุมดูแลการพัฒนาและใช้งานปัญญาประดิษฐ์สามารถตรวจสอบกิจกรรมต่าง ๆ ว่าดำเนินไปด้วยความถูกต้อง และสามารถคาดการณ์การกระทำต่าง ๆ ได้

ภาระความรับผิดชอบ (Accountability) หมายถึง ภาระความรับผิดชอบที่มี หากเกิด ผลกระทบที่เกิดขึ้นจากปัญญาประดิษฐ์ โดยให้ผู้ที่เกี่ยวข้องกับปัญญาประดิษฐ์ เช่น ผู้วิจัย ผู้ออกแบบ ผู้พัฒนา และผู้ใช้งานปัญญาประดิษฐ์รับผิดชอบเยียวยาผู้ได้รับผลกระทบเฉพาะที่เกิดจากขอบเขตภาระหน้าที่เฉพาะส่วนของตนเท่านั้น

ความสามารถในการสืบย้อน (Traceability) หมายถึง ความสามารถในการตรวจสอบย้อนกลับไปตั้งแต่แหล่งที่มาของชุดข้อมูล กระบวนการทำงาน และการตัดสินใจของปัญญาประดิษฐ์ เพื่อใช้ในการเฝ้าระวัง ตรวจสอบความผิดปกติที่พบและสามารถวินิจฉัยปัญหาที่ทำให้เกิดความผิดพลาดล้มเหลวได้

ความมั่นคงปลอดภัย (Security) หมายถึง การสร้างความมั่นคงปลอดภัยให้แก่ปัญญาประดิษฐ์ โดยอาจใช้นโยบายและมาตรฐานทางเทคนิคด้านความมั่นคงปลอดภัย การเฝ้าระวัง การประเมิน และจัดการความเสี่ยง การคุ้มครองความเป็นส่วนตัว สำหรับการวิจัย ออกแบบ พัฒนา และใช้งานปัญญาประดิษฐ์ เพื่อลดช่องโหว่และป้องกันภัยคุกคามของปัญญาประดิษฐ์ที่ก่อให้เกิดผลกระทบในด้านลบ รวมถึงผลกระทบด้านจริยธรรม ชีวิตและสิ่งแวดล้อม และให้ผู้วิจัย ผู้ออกแบบ ผู้พัฒนาและผู้ให้บริการปฏิบัติตาม

ความเป็นส่วนตัว (Privacy) หมายถึง ข้อมูลส่วนบุคคลที่เป็นสิทธิเสรีภาพส่วนบุคคลของมนุษย์ ซึ่งหากต้องการนำข้อมูลส่วนบุคคลของผู้ใดไปใช้งาน จะต้องไม่ดำเนินการขัดกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยต้องทำการแจ้งให้ผู้ใช้งานปัญญาประดิษฐ์ทราบเป็นการล่วงหน้าถึงข้อมูลที่จะถูกเก็บรวบรวมและการนำไปใช้ และข้อมูลส่วนบุคคลดังกล่าวต้องได้รับการยินยอมจากเจ้าของข้อมูลเสียก่อน

ความเป็นธรรม (Fairness) หมายถึง ความเท่าเทียมกันทางด้านโอกาสในสังคม โดยผู้ที่จะได้รับประโยชน์จากปัญญาประดิษฐ์ ควรเป็นประชาชนทุกคน รวมถึงกลุ่มคนด้อยโอกาส เช่น ผู้พิการ และผู้ทุพพลภาพด้วย

ความน่าเชื่อถือ (Reliability) หมายถึง คุณภาพของปัญญาประดิษฐ์ในด้านต่าง ๆ ที่ส่งผลให้เกิดความเชื่อถือต่อผู้ใช้งานปัญญาประดิษฐ์ เช่น ความถูกต้องแม่นยำ ความสมบูรณ์ ความเป็นปัจจุบัน ความเกี่ยวข้องของข้อมูล ความครบถ้วนถูกต้อง การคาดการณ์ได้ถูกต้องแม่นยำ และความสามารถในการนำไปใช้

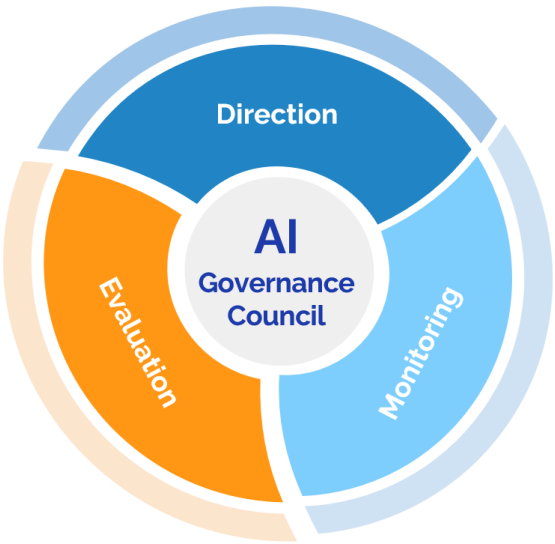
1 ธรรมาภิบาลในการประยุกต์ใช้ AI (AI Governance) และหลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles)

1.1 ธรรมาภิบาลในการประยุกต์ใช้ AI (AI Governance)

ธรรมาภิบาลในการประยุกต์ใช้ AI คือ **หลักการกำกับดูแลการปฏิบัติงานในทุกกระบวนการที่เกี่ยวข้องกับการประยุกต์ใช้ AI โดยจัดให้มีมาตรการในการกำกับดูแลผ่านการกำหนดนโยบาย ขั้นตอนปฏิบัติ และเครื่องมือในการปฏิบัติงาน เพื่อให้มั่นใจว่าการประยุกต์ใช้ AI นั้น สามารถบรรลุตามเป้าหมายขององค์กรอย่างมีความรับผิดชอบ** โดยคำนึงถึงความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ ความสอดคล้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง และมีการควบคุมความเสี่ยงที่อาจส่งผลกระทบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังคมโดยกว้าง

โดยมีคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) ซึ่งมีหน้าที่หลัก ดังนี้

1) **กำหนดทิศทางการดำเนินการ (Direction)** โดยกำหนดกลยุทธ์ในการประยุกต์ใช้ AI และนโยบายที่เกี่ยวข้องเพื่อขับเคลื่อนการประยุกต์ใช้ AI
2) **เฝ้าติดตาม (Monitoring) ประสิทธิภาพ (Performance)** ของการประยุกต์ใช้ AI รวมถึงการปฏิบัติงานตามนโยบายและข้อกำหนดต่าง ๆ (Conformance) ทั้งภายในและภายนอกองค์กร
3) **ประเมินผล (Evaluation)** การประยุกต์ใช้งาน AI ในปัจจุบันและอนาคต โดยพิจารณาจากปัจจัยที่เกี่ยวข้องทั้งภายในและภายนอก เช่น เป้าหมายในการประยุกต์ใช้ AI ภัยคุกคามและโอกาสจากการประยุกต์ใช้ AI ความเปลี่ยนแปลงด้านเทคโนโลยี ประสิทธิภาพและประสิทธิผลในการกำกับดูแล เป็นต้น



1.2 หลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles)

เพื่อให้การประยุกต์ใช้ AI เป็นไปอย่างมีความรับผิดชอบนั้น จำเป็นต้องมีการนำหลักการจริยธรรม AI ที่เกี่ยวข้องมาปรับใช้ โดยองค์กรจะต้องกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) และนโยบายให้สอดคล้องตามหลักการจริยธรรมที่เกี่ยวข้อง ซึ่งในการพิจารณานำหลักการจริยธรรม AI มาปรับใช้นั้นขึ้นอยู่กับบริบทขององค์กร

ทั้งนี้ องค์กรพิจารณานำหลักการจริยธรรมปัญญาประดิษฐ์ตามแนวทางของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) มาปรับใช้ทั้งหมดหรือบางส่วน หรืออาจนำหลักจริยธรรมปัญญาประดิษฐ์อื่น ๆ ที่เกี่ยวข้องกับบริบทของการประยุกต์ใช้ AI มาปรับใช้ตามความเหมาะสม

1) **ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน (Competitiveness and Sustainability Development)** AI ควรถูกสร้างและใช้งานเพื่อสร้างประโยชน์และความผาสุกให้แก่มนุษย์ สังคม เศรษฐกิจ และสิ่งแวดล้อมอย่างยั่งยืน รวมถึงเพิ่มความสามารถในการแข่งขันและสร้างความเจริญให้กับทุกภาคส่วนในโลกอย่างเป็นธรรม นอกจากนี้ AI ยังควรได้รับการวิจัยและพัฒนาอย่างต่อเนื่อง เพื่อสร้างสรรค์นวัตกรรมและอุตสาหกรรมใหม่

2) **ความสอดคล้องกับกฎหมาย จริยธรรม และมาตรฐานสากล (Laws Ethics and International Standards)** AI ควรได้รับการออกแบบ พัฒนาให้บริการ และใช้งาน โดยสอดคล้องกับกฎหมาย บรรทัดฐาน จริยธรรม คุณธรรมของมนุษย์ และมาตรฐานสากล โดยเคารพต่อความเป็นส่วนตัว เกียรติ สิทธิเสรีภาพ และสิทธิมนุษยชน นอกจากนี้ AI ยังควรได้รับการออกแบบโดยมีมนุษย์เป็นศูนย์กลาง และเป็นผู้ตัดสินใจ (Human-Centered Design) และไม่ควรถูกใช้ในการกำหนดชะตาชีวิตของมนุษย์

3) **ความโปร่งใสและภาระความรับผิดชอบ (Transparency and Accountability)** AI ควรได้รับการออกแบบพัฒนาให้บริการ และใช้งานด้วยความโปร่งใส สามารถอธิบาย (Explainability) และคาดการณ์ผลลัพธ์จากการทำงานได้ อีกทั้ง ยังควรมีการเฝ้าติดตามความผิดปกติ มีความสามารถในการสืบย้อนกลับ (Traceability) และสามารถวินิจฉัยปัญหาและความผิดพลาดได้ (Diagnosability) นอกจากนี้ องค์กรยังควรมีการกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงความรับผิดชอบต่อผลของการกระทำ (Accountability) ต่อผลกระทบที่เกิดขึ้นจาก AI ตามหน้าที่ที่รับผิดชอบได้

4) **ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)** AI ควรถูกออกแบบและพัฒนาโดยให้ความสำคัญถึงความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัว โดยจัดให้มีมาตรการป้องกันการโจมตีทางไซเบอร์ และปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงกลไกที่ให้มนุษย์สามารถแทรกแซงเพื่อควบคุมการทำงานของ AI ในกรณีที่เกิดเหตุการณ์หรือความเสี่ยงที่มีผลกระทบกับมนุษย์ได้

5) **ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)** ในการส่งเสริมการประยุกต์ใช้ AI อย่างเป็นธรรม และลดความมีอคติ (Bias) ระบบควรถูกออกแบบและพัฒนาโดยคำนึงถึงความหลากหลาย (Diversity) ลดการเอนเอียง แบ่งแยก และเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มคนที่มีคุณลักษณะที่ต่างกัน (อาทิเช่น อายุ เพศ ลักษณะทางกายภาพ เชื้อชาติ) โดยเฉพาะกลุ่มคนผู้ด้อยโอกาสในสังคม รวมถึงสามารถพิสูจน์ถึงความเป็นธรรมสำหรับทุกฝ่ายที่เกี่ยวข้อง

6) **ความน่าเชื่อถือ (Reliability)** AI ควรได้รับการสนับสนุนให้มีความน่าเชื่อถือและความมั่นใจในการใช้งานต่อสาธารณะ โดยสนับสนุนให้มีการพัฒนาด้วยความยึดมั่นในความถูกต้อง (Accuracy) ความน่าเชื่อถือ (Reliability) สามารถทนทานต่อเหตุการณ์ที่อาจเกิดความผิดพลาด (Robustness) และสามารถสร้างผลลัพธ์ได้เหมือนเดิม (Reproducibility) นอกจากนี้ควรมีการควบคุมคุณภาพของข้อมูล (Quality of data) รวมถึงกำหนดกระบวนการและช่องทางรับความคิดเห็น (Feedback) จากผู้ใช้งาน ให้ข้อมูลเพิ่มเติม รับเรื่องร้องเรียน แจ้งปัญหาที่พบ และมีการตอบสนองหรือดำเนินการแก้ไขปัญหาที่พบได้ทันท่วงที

2 กรอบการทำงานเพื่อสนับสนุนให้เกิดธรรมาภิบาลในการประยุกต์ใช้ AI ประกอบด้วย 3 องค์ประกอบหลัก ได้แก่

1) <u>AI Governance Structure</u>
   - จัดตั้งคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) เพื่อกำหนดทิศทางการประยุกต์ใช้งาน AI ผ่านการกำหนดกลยุทธ์และนโยบาย รวมถึง เฝ้าติดตาม และประเมินผลการประยุกต์ใช้ AI อย่างต่อเนื่อง เพื่อสนับสนุนให้เกิดธรรมาภิบาลในการประยุกต์ใช้ AI
   - กำหนดหน้าที่ของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการประยุกต์ใช้ AI พร้อมทั้งสร้างความตระหนักรู้ในด้านความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability) ของแต่ละหน้าที่
   - พัฒนาศักยภาพของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานได้อย่างเหมาะสมตามหน้าที่ที่ได้รับมอบหมาย
2) <u>AI Strategy</u>
   - มองหาโอกาสในการนำ AI มาประยุกต์ใช้ เพื่อสนับสนุนให้บรรลุเป้าหมายขององค์กรหรือเป้าหมายทางธุรกิจ
   - กำหนดเป้าหมายในการประยุกต์ใช้ AI ตามลำดับความสำคัญ โดยพิจารณาจากประโยชน์ที่จะได้รับ ความพร้อมขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่ต้องดำเนินการให้สอดคล้อง รวมถึงความซับซ้อนและเวลาที่จำเป็นต้องใช้ในการดำเนินการ
   - กำหนดกลยุทธ์ในการบริหารจัดการข้อมูล
   - กำหนดแผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap)
   - วิเคราะห์ความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI รวมถึงการกำหนดระดับการมีส่วนร่วมของมนุษย์ในการทำงานของ AI และมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้
3) <u>AI Operation</u>
   - จัดทำข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) พร้อมทั้งออกแบบโซลูชั่นที่เหมาะสมกับข้อกำหนดดังกล่าว
   - จัดเตรียมข้อมูลที่มีคุณภาพสำหรับการสอน ตรวจสอบ และทดสอบโมเดลปัญญาประดิษฐ์ รวมถึงลดความมีอคติที่อาจเกิดจากข้อมูล (Data Bias)
   - สร้างโมเดล AI โดยนำหลักการจริยธรรมปัญญาประดิษฐ์มาปรับใช้ และควบคุมความเสี่ยงที่อาจเกิดขึ้น
   - เฝ้าติดตามประสิทธิภาพ (Performance) การประยุกต์ใช้ AI รวมถึงการปฏิบัติงานตามนโยบาย หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง (Compliance)
   - ประเมินผลการประยุกต์ใช้งาน AI ในปัจจุบันและกำหนดแนวทางการดำเนินงานอนาคต

ตารางแสดงความสัมพันธ์ระหว่างหลักการจริยธรรมปัญญาประดิษฐ์และองค์ประกอบในการสนับสนุนธรรมาภิบาลในการประยุกต์ใช้ AI

หลักการจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles)	องค์ประกอบในการสนับสนุนธรรมาภิบาลในการประยุกต์ใช้ AI		
	การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure)	การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)	การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)
ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน (Competitiveness and Sustainability Development)	✓	✓	
ความสอดคล้องกับกฎหมาย จริยธรรม และมาตรฐานสากล (Laws Ethics and International Standards)	✓	✓	✓
ความโปร่งใสและภาระความรับผิดชอบ (Transparency and Accountability)	✓		✓
ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)			✓
ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)			✓
ความน่าเชื่อถือ (Reliability)			✓

3 การกำหนดโครงสร้างการกำกับดูแล (AI Governance Structure)

3.1 คณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council)

ในการประยุกต์ใช้ AI อย่างมีธรรมาภิบาลนั้น องค์กรจำเป็นต้องมีการกำหนดโครงสร้างการกำกับดูแลภายในองค์กร โดยมีการกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงกำหนดความรับผิดชอบต่อผลของการกระทำ (Accountability) ของบุคลากรภายในองค์กร และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องตามหน้าที่ที่ได้รับมอบหมาย เพื่อให้มั่นใจได้ว่าการประยุกต์ใช้ AI จะเป็นไปตามเป้าหมาย สอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ พร้อมทั้งมีการควบคุมความเสี่ยงที่อาจเกิดขึ้น โดยมีคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council) เป็นศูนย์กลางในการกำหนดทิศทางการดำเนินการ (Direction) การเฝ้าติดตาม (Monitoring) และการประเมินผล (Evaluation) การประยุกต์ใช้ AI

คณะกรรมการกำกับดูแลฯ เป็นผู้รับผิดชอบโดยตรง ต่อผลลัพธ์จากการทำงานหรือการตัดสินใจของ AI ดังนั้น จึงจำเป็นต้องมีการกำกับดูแลเพื่อให้มั่นใจได้ว่า การประยุกต์ใช้ AI เป็นไปตามเป้าหมายที่กำหนด สอดคล้องตาม หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนด ที่เกี่ยวข้อง รวมถึงควบคุมความเสี่ยง ให้อยู่ในขอบเขตที่ยอมรับได้

3.1.1 การกำหนดทิศทางการดำเนินการ (Direction)

พิจารณากลยุทธ์การประยุกต์ใช้ AI (AI Strategy) รวมถึงกำหนดนโยบายที่เกี่ยวข้องกับการประยุกต์ใช้ AI และการกำกับดูแล (AI Governance Policies) ในด้านต่าง ๆ เช่น

- โครงสร้างการกำกับดูแล
- หน้าที่และความรับผิดชอบ และความรับผิดชอบต่อผลของการกระทำ
- การบริหารจัดการและการใช้งานข้อมูล
- การออกแบบโซลูชั่น สร้าง ทดสอบ และนำ AI ไปประยุกต์ใช้งาน
- การทำงานร่วมกันระหว่าง AI กับมนุษย์
- การประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI
- การอนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ เช่น แผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap) การนำโมเดลปัญญาประดิษฐ์ (AI Model) ไปใช้งานจริง ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ การแก้ไขประเด็นปัญหาและแนวทางการดำเนินงานที่เกี่ยวข้องกับการประยุกต์ใช้ AI เป็นต้น

พร้อมทั้ง มีหน้าที่ในการสื่อสารนโยบายและทิศทางของการกำกับดูแลให้แก่บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องเพื่อให้เกิดความเข้าใจและรับทราบร่วมกัน

นอกจากนี้ ในด้านของการควบคุมความเสี่ยง คณะกรรมการกำกับดูแลฯ ยังมีหน้าที่ในการพิจารณาว่าความเสี่ยงใดเป็นความเสี่ยงที่ ยอมรับได้ (Risk Appetite) พร้อมทั้งกำกับดูแลให้มีการบริหารจัดการความเสี่ยง (Risk Management) อย่างเหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

3.1.2 การเฝ้าติดตาม (Monitoring)

เฝ้าติดตามประสิทธิภาพของการประยุกต์ใช้ AI (Performance) รวมถึงเฝ้าติดตามการปฏิบัติงานตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ (Conformance) และเฝ้าติดตามความเสี่ยงว่ายังอยู่ในระดับยอมรับได้

โดย**เฝ้าติดตามจากรายงานผลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง** โดยรายงานอาจประกอบด้วยข้อมูล เช่น

- ผลการดำเนินงานตามตัวชี้วัดที่องค์กรกำหนด (Key Performance Indicator: KPI)
- รายงานข้อมูลเกี่ยวกับความถูกต้องของการตัดสินใจของ AI
- ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ที่เกี่ยวข้อง
- ข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) ที่พบจากการประยุกต์ใช้ AI

ทั้งนี้ การรายงานผลการปฏิบัติงานต่อคณะกรรมการกำกับดูแลฯ อย่างทันท่วงทีและมีข้อมูลที่เพียงพอต่อการตัดสินใจ จะช่วยสร้างความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้อง

3.1.3 การประเมินผล (Evaluation)

ควรมีการประเมินผลการปฏิบัติงาน และประเมินผลการประยุกต์ใช้งาน AI ที่ผ่านมา เพื่อพิจารณาสิ่งที่ต้องปรับปรุงและกำหนดแนวทางการดำเนินงานในอนาคต โดยในการประเมินผลการประยุกต์ใช้ AI นั้น องค์กรอาจจัดให้มีการประเมินผลโดยผู้ตรวจประเมินภายใน (Internal Auditor) หรือผู้ตรวจประเมินภายนอก (External Auditor) ตามความเหมาะสม เพื่อช่วยเพิ่มความน่าเชื่อถือ (Reliability) และสร้างการยอมรับจากบุคคลที่เกี่ยวข้อง

โดยในการประเมินผลการประยุกต์ใช้งานนั้น อาจมีการพิจารณาในด้านต่าง ๆ ตัวอย่างเช่น

- ประเมินประสิทธิภาพในการทำงานของ AI และผลลัพธ์ความสำเร็จจากการประยุกต์ใช้ AI ที่ผ่านมาเมื่อเทียบกับเป้าหมายที่กำหนด
- พิจารณาปรับปรุงเป้าหมายในการประยุกต์ใช้ AI หากพบว่าการประยุกต์ใช้ AI ไม่สามารถช่วยให้องค์กรบรรลุเป้าหมายตามที่กำหนดได้
- พิจารณาปรับปรุงข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) หากพบว่าข้อกำหนดความต้องการไม่ถูกต้อง หรือยกเลิกข้อกำหนดในบางเรื่องหากพบว่าไม่มีความจำเป็น
- นำความคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) ที่พบ มาพิจารณาปรับปรุงเป้าหมายในการประยุกต์ใช้หรือข้อกำหนดความต้องการในการพัฒนาระบบ
- ประเมินประสิทธิภาพของมาตรการในการกำกับดูแล เพื่อให้การประยุกต์ใช้ AI สอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้อง
- ทบทวนความเสี่ยงจากการดำเนินงานที่ผ่านมา รวมถึงวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นในอนาคต เพื่อกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite) รวมถึงปรับปรุงมาตรการในการควบคุมความเสี่ยงและแผนการจัดการความเสี่ยง (Risk Treatment Plan) ให้เหมาะสม

การจัดตั้งคณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (Setting up AI Governance Council)

เนื่องจากคณะกรรมการกำกับดูแลฯ เป็นศูนย์กลางในการกำกับดูแลการประยุกต์ใช้ AI จึงอาจสรุปหน้าที่และความรับผิดชอบหลักในการกำกับดูแล ได้ดังนี้

1) กำกับดูแลการปฏิบัติงานเพื่อให้การประยุกต์ใช้ AI ประสบความสำเร็จและบรรลุตามเป้าหมายที่องค์กรกำหนด ผ่านการกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy) และการกำหนดนโยบาย
2) เฝ้าติดตามประสิทธิภาพ (Performance) และประเมินผลการประยุกต์ใช้ AI
3) เฝ้าติดตามและประเมินผลการปฏิบัติงานให้สอดคล้อง (Conformance) ตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง
4) กำกับดูแลและควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้
5) อนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ ที่เกี่ยวข้องกับการประยุกต์ใช้ AI

3.2 หน้าที่และความรับผิดชอบ (Role and Responsibility)

การกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงกำหนดความรับผิดชอบต่อผลของการกระทำ (Accountability) ของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในทุกกระบวนการของการประยุกต์ใช้ AI โดยอาจสรุปได้ ดังนี้

3.2.1 ระดับนโยบาย (Strategic Level)

อาจประกอบด้วย:

- ผู้บริหารระดับสูง
- คณะกรรมการจริยธรรม*
- คณะกรรมการตามโครงสร้าง GRC*
- คณะกรรมการธรรมาภิบาลข้อมูล*
- ผู้บริหารหรือผู้แทนจากทีมงานภายในองค์กรที่เกี่ยวข้องกับการประยุกต์ใช้ AI
- ผู้เชี่ยวชาญหรือหน่วยงานกำกับดูแล**

หมายเหตุ:

* โครงสร้างการกำกับดูแลภายในองค์กรที่อาจนำมาปรับใช้เพื่อสนับสนุนหรือร่วมดำเนินงาน

** บุคคลหรือกลุ่มบุคคลภายนอกที่อาจเข้ามาร่วมดำเนินงาน

<u>ด้านกำกับดูแลการปฏิบัติงานเพื่อบรรลุเป้าหมายที่กำหนด</u>

- กำหนดกลยุทธ์และเป้าหมายในการประยุกต์ใช้ AI ภายในองค์กร
- กำหนดนโยบายที่เกี่ยวข้องกับการประยุกต์ใช้ AI และนโยบายในการกำกับดูแลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
- อนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ ที่เกี่ยวข้องกับการประยุกต์ใช้ AI เช่น
  - แผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap)
  - การนำโมเดลปัญญาประดิษฐ์ (AI Model) ไปใช้งานจริง
  - ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์

- การแก้ไขประเด็นปัญหาและกำหนดแนวทางการดำเนินงาน

- เฝ้าติดตามประสิทธิภาพการทำงานของ AI และระดับความสำเร็จในการประยุกต์ใช้ AI เมื่อเทียบกับเป้าหมายที่กำหนด
- ประเมินผลประยุกต์ใช้งาน AI ที่ผ่านมาและกำหนดแนวทางการดำเนินงานในอนาคต

ด้านการปฏิบัติงานให้สอดคล้อง (Conformance) ตามข้อกำหนดภายในและภายนอกองค์กร

- กำหนดนโยบายในการกำกับดูแลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง รวมถึงเฝ้าติดตามและประเมินผลการปฏิบัติงานตามนโยบายองค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง

ด้านการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- กำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite) และพิจารณาความเหมาะสมของมาตรการเพื่อจำกัดความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

นอกจากการกำหนดหน้าที่และความรับผิดชอบดังกล่าวข้างต้น องค์กรยังจำเป็นต้องมี**การสื่อสารนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้อง พร้อมทั้งสร้างความตระหนักรู้ (Awareness) ต่อความรับผิดชอบ (Responsibility) และความรับผิดชอบต่อผลของการกระทำ (Accountability)**

ในกรณีที่มีการว่าจ้างหน่วยงานภายนอก (Outsource) เช่น หน่วยงานที่รับจ้างพัฒนาระบบ (Vendor) ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) เป็นต้น **องค์กรยังคงต้องมีความรับผิดชอบต่อผลของการกระทำ (Accountability) อันเกิดจากการทำงานของ AI** ด้วยเหตุนี้ **องค์กรควรมีการกำกับดูแลการปฏิบัติงานของหน่วยงานภายนอกอย่างเหมาะสม พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบในข้อตกลงว่าจ้างหรือข้อตกลงการใช้บริการ**

3.3 การพัฒนาศักยภาพบุคลากร (Competency Building)

เพื่อให้องค์กรประสบความสำเร็จในการประยุกต์ใช้ AI **คณะกรรมการกำกับดูแลฯ รวมถึงบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ควรได้รับการส่งเสริมให้มีความรู้ความเข้าใจเกี่ยวกับ AI ในมิติต่าง ๆ อย่างเหมาะสมตามหน้าที่ที่ได้รับมอบหมาย** เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างถูกต้องและสอดคล้องตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง รวมถึงสามารถรับมือกับความเสี่ยงและเหตุการณ์ผิดปกติได้อย่างเหมาะสม

ตัวอย่าง องค์ความรู้ที่เกี่ยวกับการประยุกต์ใช้ AI

4 การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)

4.1 การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ (Responsible AI Strategy)

ปัจจุบันเทคโนโลยี AI ถูกนำมาประยุกต์ใช้ในรูปแบบที่หลากหลายแตกต่างกันตามวัตถุประสงค์หรือเป้าหมายขององค์กร เพื่อให้การประยุกต์ใช้ AI ประสบความสำเร็จและบรรลุตามเป้าหมาย องค์กรจึงควรกำหนดกลยุทธ์ในการประยุกต์ใช้ AI และแผนปฏิบัติงานอย่างเหมาะสม โดย**พิจารณาถึงโอกาสหรือประโยชน์ที่องค์กรจะได้รับและพิจารณาความเป็นไปได้ในการประยุกต์ใช้ AI**

โดยพิจารณาความเป็นไปได้นั้น องค์กรควรพิจารณาถึงปัจจัยในด้านต่าง ๆ เช่น ความสามารถของเทคโนโลยีและผลิตภัณฑ์ในปัจจุบันที่สามารถตอบโจทย์ความต้องการขององค์กร ความพร้อมของข้อมูลและทรัพยากรที่เกี่ยวข้อง ความซับซ้อนและเวลาที่ใช้ดำเนินการ ข้อจำกัดและความท้าทายในการดำเนินงาน เป็นต้น

นอกจากนี้ เพื่อให้เกิดการประยุกต์ใช้งาน AI อย่างมีความรับผิดชอบ ในการกำหนดกลยุทธ์ยังจำเป็นต้องมี**การพิจารณาและคาดการณ์ถึงผลกระทบเชิงลบที่อาจส่งผลกระทบต่อบุคคลที่เกี่ยวข้อง องค์กร หรือสังคมโดยกว้าง** เช่น การตัดสินใจของ AI ที่มีอคติจนนำไปสู่การเลือกปฏิบัติ การทำงานที่ผิดพลาดของ AI ก่อให้เกิดความเสียหายต่อชื่อเสียง ชีวิต หรือทรัพย์สิน เป็นต้น ด้วยเหตุนี้ องค์กรจึงควรมีการกำหนดกลยุทธ์และจัดทำแผนปฏิบัติงาน เพื่อให้ระบบหรือบริการที่เกี่ยวข้องกับ AI ทำงานได้อย่างสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นดังกล่าว

4.1.1 มองหาโอกาสในการนำ AI มาประยุกต์ใช้

เพื่อให้เห็นโอกาสในการนำ AI มาประยุกต์ใช้ องค์กรจึงควรเริ่มต้นจาก**การทำความเข้าใจภาพรวม วิสัยทัศน์ พันธกิจ รวมถึงเป้าหมายระยะสั้นและระยะยาวขององค์กร เพื่อเข้าใจเป้าหมายขององค์กรหรือเป้าหมายในการดำเนินธุรกิจ จากนั้นจึงเริ่มทำการวิเคราะห์กระบวนการหรือขั้นตอนปฏิบัติต่าง ๆ เพื่อมองหาโอกาสที่ AI จะเข้ามาเป็นองค์ประกอบหนึ่งในการทำงาน ซึ่งจะช่วยให้องค์กรบรรลุตามเป้าหมายหรือตอบโจทย์ความต้องการทางธุรกิจได้อย่างมีประสิทธิภาพมากยิ่งขึ้น** โดยในการวิเคราะห์นั้นอาจพิจารณาในประเด็นดังต่อไปนี้

- **ประโยชน์ที่องค์กรจะได้รับจากการนำ AI มาประยุกต์ใช้** เช่น เพิ่มรายได้ให้แก่องค์กร การยกระดับความพึงพอใจของลูกค้า ปรับปรุงประสิทธิภาพและผลิตผล ลดค่าใช้จ่ายในการปฏิบัติงาน เป็นต้น
- **ระดับความสำเร็จที่คาดหวังว่า** AI จะเข้ามาช่วยให้องค์กรบรรลุเป้าหมายในการดำเนินธุรกิจ หรือความสำเร็จตามตัวชี้วัดที่องค์กรกำหนด (Key Performance Indicator: KPI) เช่น สามารถช่วยลดค่าใช้จ่ายลงได้ 20% สามารถผลิตสินค้าได้มากขึ้น 500 ชิ้น/วัน
- **เทคโนโลยีและวิธีการที่จะนำ AI มาประยุกต์ใช้**
- **ขอบเขตการดำเนินงาน**ที่ AI จะเข้าไปเกี่ยวข้องกับการปฏิบัติงาน
- **ข้อมูลและทรัพยากรที่จำเป็น**ต้องใช้ในการดำเนินการ เช่น งบประมาณ บุคลากร โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นต้น

- **ผลกระทบจากการนำ AI ไปประยุกต์ใช้** เช่น การปรับเปลี่ยนกระบวนการหรือขั้นตอนปฏิบัติงาน ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย ความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้งาน AI และมาตรการในการควบคุมความเสี่ยงและผลกระทบ เป็นต้น
- **ข้อจำกัดหรือความท้าทายในการประยุกต์ใช้ AI** เช่น กฎหมายและข้อกำหนดที่ต้องปฏิบัติตามข้อจำกัดด้านทรัพยากร ปริมาณและคุณภาพของข้อมูลที่มีอยู่ในปัจจุบัน เป็นต้น

โดยในการวิเคราะห์กระบวนการหรือขั้นตอนปฏิบัติต่าง ๆ นั้น **ควรมีการทำงานร่วมกันระหว่างผู้เชี่ยวชาญด้าน AI และทีมงานด้านธุรกิจหรือผู้ที่เกี่ยวข้องกับการปฏิบัติงานโดยตรง** เพื่อสะท้อนมุมมองในทางปฏิบัติและวิเคราะห์ความเป็นไปได้ในการที่จะนำ AI มาประยุกต์ใช้

4.1.2 กำหนดเป้าหมายในการประยุกต์ใช้ AI

ภายหลังจากทำการวิเคราะห์กระบวนการหรือขั้นตอนปฏิบัติเพื่อมองหาโอกาสและความเป็นไปได้ที่จะนำ AI มาประยุกต์ใช้นั้น องค์กรอาจพบว่ามีกระบวนการหรือขั้นตอนปฏิบัติจำนวนมาก หลากหลาย และอาจไม่สามารถดำเนินการไปพร้อมกันได้ทั้งหมด ด้วยเหตุนี้ **องค์กรจึงจำเป็นต้องจัดลำดับความสำคัญในการดำเนินงาน** โดยอาจพิจารณาจากปัจจัยต่าง ๆ ได้แก่

- **ประโยชน์ที่องค์กรจะได้รับ**จากการนำ AI มาประยุกต์ใช้ในกระบวนการหรือขั้นตอนปฏิบัตินั้น
- **ระดับความสำเร็จที่คาดหวัง**ว่า AI จะเข้ามาช่วยให้บรรลุเป้าหมายขององค์กร เป้าหมายในการดำเนินธุรกิจ หรือความสำเร็จตามตัวชี้วัดที่องค์กรกำหนด (Key Performance Indicator: KPI)
- **หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมาย และข้อกำหนด** ที่ต้องออกแบบและพัฒนาระบบให้สอดคล้อง
- **ความพร้อมของทรัพยากร**ที่จำเป็นต้องใช้ในการดำเนินการ เช่น งบประมาณ ข้อมูล บุคลากร โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นต้น
- **ความพร้อมในการกำกับดูแลและการปฏิบัติงาน**เพื่อเปลี่ยนผ่านไปสู่การนำ AI มาประยุกต์ใช้จริง รวมถึงการรับมือความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- **ความซับซ้อนและเวลาที่ใช้**ในการดำเนินการ

ซึ่งการจัดลำดับความสำคัญในการดำเนินงานดังกล่าว จะช่วยให้องค์กรสามารถเลือกเป้าหมายในการประยุกต์ใช้งาน AI ตามลำดับความสำคัญ และสามารถจัดสรรทรัพยากรได้อย่างมีประสิทธิภาพ

4.1.3 กำหนดกลยุทธ์ในการบริหารจัดการข้อมูลเพื่อสนับสนุนการประยุกต์ใช้ AI

ข้อมูล คือ อาหารของ AI
หากองค์กรใช้ข้อมูลที่ไม่มีคุณภาพในการสอน AI
ผลลัพธ์จากการทำงาน หรือการตัดสินใจของ AI
ก็จะไม่มีคุณภาพเช่นกัน

เนื่องจาก AI จำเป็นต้องใช้ข้อมูลในการประมวลผล ด้วยเหตุนี้ องค์กรจึงจำเป็นต้องมีการ**กำหนดกลยุทธ์ในการบริหารจัดการข้อมูลอย่างเหมาะสม ตั้งแต่กระบวนการสรรหาแหล่งข้อมูลที่เหมาะสม การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่พร้อมใช้งานและเพียงพอสำหรับ AI ในการประมวลผล ไปจนถึงการพัฒนาอัลกอริทึมให้สามารถทำงานได้อย่างมีประสิทธิภาพบนพื้นฐานของข้อมูลที่มีอยู่**

เพื่อให้มั่นใจได้ว่าองค์กรจะมีข้อมูลที่เหมาะสมและเพียงพอต่อการสนับสนุนการประยุกต์ใช้ AI ให้บรรลุตามเป้าหมายที่กำหนด **องค์กรควรมีการสรรหาแหล่งข้อมูลที่เหมาะสม** โดยอาจพิจารณาจากคุณภาพของข้อมูล ความน่าเชื่อถือในการเก็บรวบรวมข้อมูล ความสามารถในการเข้าถึงข้อมูลได้โดยสะดวก ข้อมูลอยู่ในรูปแบบหรือประเภทที่ตรงตามความต้องการใช้งาน ข้อมูลมีความหลากหลายและครอบคลุมตัวอย่างที่ต้องการ มีขนาดของข้อมูลหรือขนาดของกลุ่มตัวอย่างที่เหมาะสม ข้อมูลมีการปรับปรุงให้ทันสมัยอยู่เสมอ เป็นต้น

นอกจากนี้องค์กรยังจำเป็นต้องมีการ**เตรียมความพร้อมในด้านบุคลากร เครื่องมือและกระบวนการอย่างเหมาะสม** เพื่อจัดเตรียมข้อมูลที่เหมาะสมสำหรับการพัฒนา ทดสอบ และใช้งาน AI (ซึ่งจะกล่าวถึงในหัวข้อ 5.1) รวมถึง**ควรมีการกำกับดูแลโดยนำหลักการธรรมาภิบาลข้อมูล (Data Governance) มาปรับใช้** เพื่อให้มั่นใจได้ว่าข้อมูลมีคุณภาพตรงตามความต้องการในการใช้งาน

4.1.4 จัดทำแผนปฏิบัติงาน (Road Map) ในการประยุกต์ใช้ AI

ภายหลังจากที่องค์กรสามารถกำหนดเป้าหมายในการประยุกต์ใช้งาน AI รวมถึงแนวทางการบริหารจัดการข้อมูลที่สอดคล้องตามกลยุทธ์ที่วางไว้แล้ว **องค์กรควรจัดทำแผนปฏิบัติงานตามลำดับความสำคัญ พร้อมทั้งกำหนดขั้นตอนการดำเนินงานและระยะเวลาในการดำเนินงานของแต่ละเป้าหมาย** เช่น การจัดเตรียมข้อมูล การพัฒนา ทดสอบ และการนำ AI ไปใช้งาน เป็นต้น

นอกจากนี้ **องค์กรอาจกำหนดให้มีการจัดทำระบบต้นแบบ (Prototype) ก่อนนำไปขยายผลเพื่อใช้งานจริง** เพื่อทดสอบและประเมินประสิทธิภาพในการทำงานของ AI พร้อมทั้งประเมินความคุ้มค่าในการลงทุน วิเคราะห์ปัญหาและอุปสรรคที่อาจเกิดขึ้นเมื่อนำ AI ไปประยุกต์ใช้ในสภาพแวดล้อมการใช้งานจริง

4.2 การบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI (AI Risk Management)

การประยุกต์ใช้ AI อาจนำมาซึ่งโอกาสใหม่ในการดำเนินธุรกิจหรือสร้างประโยชน์ให้แก่องค์กร แต่ในขณะเดียวกันการประยุกต์ใช้ AI ก็อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคลที่เกี่ยวข้อง องค์กร และสังโดยกว้างได้เช่นกัน ด้วยเหตุนี้ ในระหว่างการกำหนดกลยุทธ์และเป้าหมายในการประยุกต์ใช้ AI นั้น **องค์กรจึงจำเป็นต้องมีการประเมินความเสี่ยงเพื่อให้เห็นถึงความไม่แน่นอนหรือโอกาสที่การประยุกต์ใช้ AI จะไม่เป็นไปตามเป้าหมายที่กำหนด รวมถึงเห็นผลกระทบเชิงลบที่อาจเกิดขึ้น**

ทั้งนี้ ความเสี่ยงจากการประยุกต์ใช้ AI นั้น มีความหลากหลายและแตกต่างกันไปตามบริบทของการประยุกต์ใช้ AI ตัวอย่างเช่น

- **ความเสี่ยงด้านคุณภาพข้อมูล (Data Quality)** เป็นความเสี่ยงที่ข้อมูลขององค์กรมีคุณภาพไม่เพียงพอจนส่งผลให้การทำงานของ AI ไม่มีประสิทธิภาพตามเป้าหมายที่กำหนดหรือทำงานผิดพลาด เป็นต้น
- **ความเสี่ยงด้านความไม่เป็นธรรมและการเลือกปฏิบัติ (Unfairness and Discrimination)** เป็นความเสี่ยงที่ผลลัพธ์จากการทำงานของ AI นำไปสู่ความไม่เป็นธรรมและการเลือกปฏิบัติ ซึ่งอาจเกิดจากอคติที่มาจาก

การออกแบบและสร้างโมเดล (Bias Introduced By Engineering Decisions) หรือเกิดจากอคติที่มาจากข้อมูล (Data Bias) เช่น การใช้ข้อมูลที่ไม่มีความหลากหลายหรือเอนเอียงมาสอน AI เป็นต้น

- **ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Attack)** เป็นความเสี่ยงที่ AI ถูกโจมตี โดยมีวัตถุประสงค์ให้ AI ทำงานผิดพลาด หยุดการทำงาน หรือเกิดการรั่วไหลของข้อมูล เป็นต้น โดยอาศัยช่องโหว่ (Vulnerability) ของระบบ AI หรือ โจมตีข้อมูลที่ใช้ในการสอน AI โดยทำให้ข้อมูลปนเปื้อนด้วยข้อมูลที่ทำให้เกิดช่องโหว่
- **ความเสี่ยงด้านการคุ้มครองความเป็นส่วนตัว (Privacy)** เป็นความเสี่ยงที่ข้อมูลส่วนบุคคลถูกละเมิด โดยอาจเกิดจากการมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เหมาะสม ความผิดพลาดในการปฏิบัติงาน หรือถูกโจมตีโดยผู้ประสงค์ร้าย เป็นต้น
- **ความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Non-Compliance)** เป็นความเสี่ยงที่ผลลัพธ์จากการทำงานของ AI นำไปสู่การละเมิดกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง
- **ความเสี่ยงด้านความน่าเชื่อถือหรือชื่อเสียง (Trust and Reputation)** เป็นความเสี่ยงที่เกิดจากการทำงานหรือการตัดสินใจของ AI ทำงานผิดพลาดหรือก่อให้เกิดผลกระทบเชิงลบ เช่น AI ทำงานผิดพลาดเมื่ออยู่ในสถานการณ์ที่ไม่เคยถูกทดสอบ หรือต้องตัดสินใจบนพื้นฐานข้อมูลที่ไม่เคยได้รับการสอนมาก่อน เป็นต้น

เพื่อลดความเสี่ยงและผลกระทบเชิงลบจากการประยุกต์ใช้งาน AI ดังกล่าว **องค์กรจึงจำเป็นต้องมีการบริหารจัดการความเสี่ยง (Risk Management) เพื่อควบคุมความเสี่ยงในทุกกิจกรรมตลอดวงจรชีวิตของ AI (AI Lifecycle) ให้อยู่ในขอบเขตที่ยอมรับได้**

4.2.1 กระบวนการในการบริหารจัดการความเสี่ยง

ในการบริหารจัดการความเสี่ยงนั้น องค์กรจำเป็นต้องมีการ**กำหนดนโยบาย กระบวนการ ขั้นตอนปฏิบัติ และมาตรการเพื่อควบคุมความเสี่ยงที่อาจเกิดขึ้นในแต่ละกิจกรรมตลอดวงจรชีวิตของ AI ซึ่งกระบวนการในการบริหารจัดการความเสี่ยงนั้น** ประกอบด้วย 6 กระบวนการหลัก ได้แก่

1) **การสื่อสารและหารือร่วมกัน (Communication and Consultation)** ระหว่างบุคลากรภายในองค์กรและผู้มีส่วนได้ส่วนเสียที่เกี่ยงข้องกับการประยุกต์ใช้ AI
2) การทำความเข้าใจขอบเขตและบริบทของการประยุกต์ใช้ AI รวมถึงกำหนด**เกณฑ์ในการประเมินความเสี่ยง (Risk Criteria)**
3) **การประเมินความเสี่ยง (Risk Assessment)** เพื่อให้องค์กรมองเห็นความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI รวมถึงมาตรการในการควบคุมความเสี่ยงดังกล่าว
4) **การกำหนดมาตรการที่เหมาะสมในการควบคุมและแก้ไขความเสี่ยง (Risk Treatment)** รวมถึงจัดทำ**แผนการดำเนินการเพื่อควบคุมและแก้ไขความเสี่ยง (Risk Treatment Plan)** ดังกล่าว เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้ นอกจากนี้ การกำหนดมาตรการในการควบคุมและแก้ไขความเสี่ยงจะต้องครอบคลุมถึงการปฏิบัติงานของหน่วยงานภายนอก เช่น หน่วยงานที่รับจ้างพัฒนาระบบ (Vendor) ผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) เป็นต้น และครอบคลุมถึงเครื่องมือหรือผลิตภัณฑ์ AI ที่ใช้งาน
5) **การเฝ้าติดตามและทบทวน (Monitoring and Review)** ประสิทธิภาพในการควบคุมและแก้ไขความเสี่ยงที่เกิดขึ้น

6) **การบันทึกและรายงานผลการบริหารจัดการความเสี่ยง (Recording & Reporting)** ต่อคณะกรรมการกำกับดูแลฯ บุคลกร และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เพื่อ**ประเมินผลการปฏิบัติงาน (Evaluation)** และปรับปรุงประสิทธิภาพในการบริหารจัดการและควบคุมการเสี่ยง

4.2.2 กรอบแนวทางการบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI (AI Risk Management Framework)

จากกระบวนการในการบริหารจัดการความเสี่ยงข้างต้น องค์กรอาจพิจารณานำกรอบแนวทางบริหารจัดการความเสี่ยงที่ประกาศโดยหน่วยงานด้านมาตรฐานสากลมาปรับใช้ โดยในปี 2023 องค์กร International Organization for Standard (ISO) ซึ่งเป็นองค์กรระหว่างประเทศด้านมาตรฐาน และสถาบัน National Institute of Standards and Technology (NIST) ซึ่งเป็นสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา ได้มีการประกาศมาตรฐาน

1) ISO/IEC 23894:2023 Information Technology – Artificial Intelligence Guidance on Risk Management ซึ่งเป็นส่วนขยาย (Extension) จากมาตรฐาน ISO 31000:2018 Risk Management – Guidelines ที่อธิบายรายละเอียดเพิ่มเติมในส่วนของการบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI
2) Artificial Intelligence Risk Management Framework (AI RMF 1.0) โดย NIST

ซึ่งทั้ง 2 มาตรฐานดังกล่าว ได้มีการวางแนวปฏิบัติในการบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI เป็นการเฉพาะ เพื่อให้องค์กรมีความเข้าใจและตระหนักถึงความเสี่ยงรูปแบบใหม่ที่เกิดจากการประยุกต์ใช้ AI รวมถึงใช้เป็นแนวทางในการรับมือกับความเสี่ยงที่จะมาเปลี่ยนแปลงสังคมและบริบทของการดำรงชีวิตของมนุษย์ในอนาคต

4.2.3 การเข้ามามีส่วนร่วมของมนุษย์ในการควบคุมการทำงานหรือตัดสินใจของ AI

การเข้ามามีส่วนร่วมของมนุษย์ในการควบคุมการทำงานหรือตัดสินใจของ AI เป็นหนึ่งใน**มาตรการที่จะช่วยควบคุมและแก้ไขความเสี่ยง (Risk Treatment) รวมถึงบรรเทาผลกระทบเชิงลบ**ที่อาจเกิดขึ้น อีกทั้งยังเป็นการสร้างความเชื่อมั่นในการประยุกต์ใช้ AI และสร้างการยอรับจากบุคคลที่เกี่ยวข้องได้

การเข้ามามีส่วนร่วมของมนุษย์ในการควบคุมการทำงานหรือตัดสินใจของ AI แบ่งได้ 3 ระดับ ได้แก่

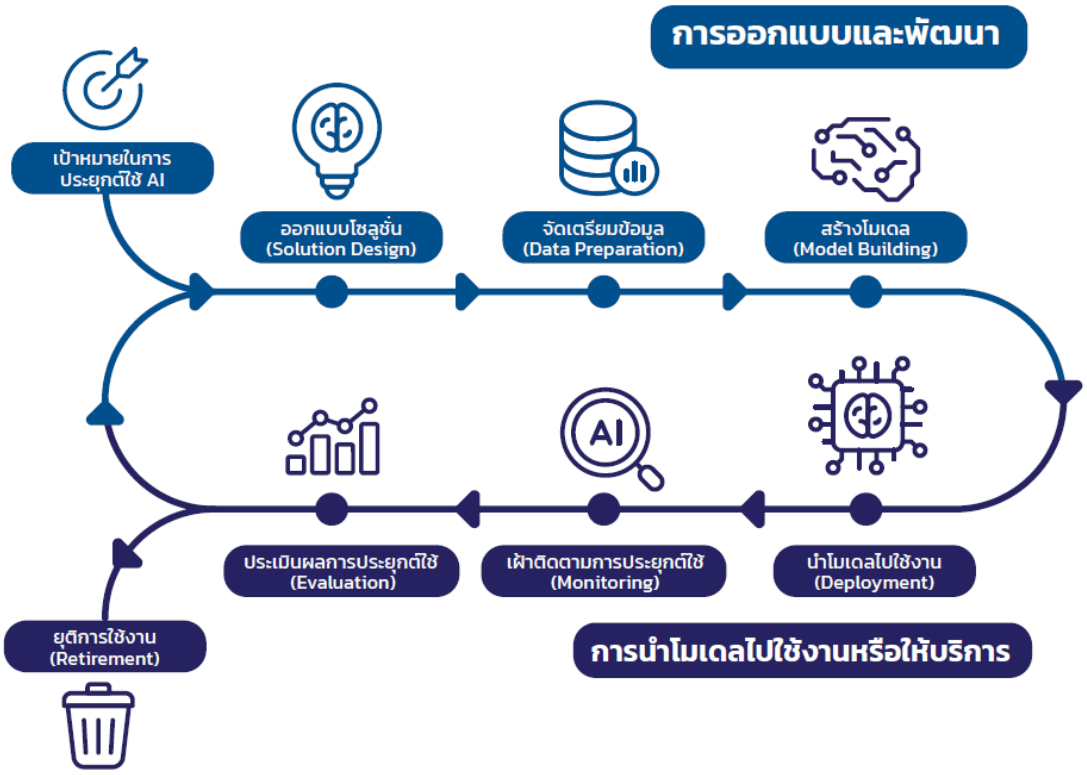
- **Human-in-the-loop** เป็นระดับการมีส่วนร่วมที่มนุษย์ควบคุมการทำงานหรือตัดสินทั้งหมด โดยมี AI ทำหน้าที่ในการให้คำแนะนำหรือหาข้อมูล แต่ไม่สามารถทำงานหรือตัดสินใจในการดำเนินการใด ๆ ได้โดยปราศจากมนุษย์
- **Human-over-the-loop** เป็นระดับการมีส่วนร่วมที่ AI สามารถทำงานหรือตัดสินได้โดยอัตโนมัติ (ไม่ต้องรอการตัดสินใจจากมนุษย์) แต่ยังคงจำเป็นต้องมีมนุษย์ในการกำกับดูแล อีกทั้งมนุษย์ยังสามารถเข้าควบคุมหรือระงับการทำงานได้ หากพบความผิดพลาดหรือเกิดเหตุการณ์ที่อาจก่อให้เกิดผลกระทบเชิงลบ
- **Human-out-of-the-loop** เป็นระดับการมีส่วนร่วมที่ AI ควบคุมการทำงานหรือตัดสินทั้งหมดได้โดยมนุษย์ไม่สามารถเข้าควบคุม แทรกแซง หรือระงับการทำงานได้ เพื่อลดผลกระทบจากความไม่พอใจในกรณีนี้ องค์กรจึงควรมีการเปิดให้มีช่องทางอื่น เพื่อให้ลูกค้าสามารถติดต่อพนักงานที่เป็นมนุษย์ได้โดยตรง

5 การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)

5.1 การกำกับดูแลตลอดวงจรชีวิตของ AI (AI Lifecycle)

ความสามารถของ AI ที่หลากหลายนั้นมีเบื้องหลังมาจากความสามารถของโมเดลปัญญาประดิษฐ์ (AI Model) (ซึ่งต่อไปในเอกสารนี้จะเรียกว่า “โมเดล”) ที่สร้างขึ้นจากอัลกอริทึมละข้อมูลที่สอนโดยมนุษย์ (เฉพาะในกรณีของ AI ประเภท Machine Learning เท่านั้น ที่จำเป็นต้องมีการเรียนรู้จากข้อมูลที่สอนโดยมนุษย์) ด้วยเหตุนี้ **ประสิทธิภาพในการประมวลผลของ AI เช่น ระดับความถูกต้อง (Accuracy) ความแม่นยำ (Precision) และระดับความน่าเชื่อถือในการตัดสินใจ (Level of Confidence) เป็นต้น จึงขึ้นอยู่กับประสิทธิภาพของอัลกอริทึมและคุณภาพของข้อมูลที่ใช้ในการสอน AI** เป็นสำคัญ

ด้วยเหตุนี้ **การกำกับดูแลการประยุกต์ใช้ AI ตลอดวงจรชีวิต (AI Lifecycle) ตั้งแต่ระยะเริ่มต้นของการออกแบบและพัฒนาไปจนถึงการนำโมเดลไปใช้งานหรือให้บริการ** จึงมีความสำคัญอย่างยิ่งในการทำให้ AI มีประสิทธิภาพสอดคล้องตามเป้าหมายที่กำหนดและมีความรับผิดชอบ ซึ่งในการกำกับดูแลนั้นควรมีการกำกับดูแลการปฏิบัติงานในกระบวนการต่าง ๆ ได้แก่ กระบวนการออกแบบโซลูชั่น จัดเตรียมข้อมูล สร้างโมเดล นำโมเดลไปใช้งาน เฝ้าติดตามและประเมินผลการประยุกต์ใช้ AI ไปจนถึงยุติการใช้งาน



5.1.1 ออกแบบโซลูชั่น (Solution Design)

เพื่อให้การประยุกต์ใช้ AI บรรลุตามเป้าหมายขององค์อย่างมีความรับผิดชอบ **องค์กรจำเป็นต้องวิเคราะห์ (1) เป้าหมายในการประยุกต์ใช้ AI (2) หลักการจริยธรรมปัญญาประดิษฐ์ (3) กฎหมายและข้อกำหนดที่เกี่ยวข้อง และ (4) มาตรการในการควบคุมและแก้ไขความเสี่ยง เพื่อนำมากำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement)** พร้อมทั้งเลือกใช้เครื่องมือหรือผลิตภัณฑ์ที่สามารถตอบสนองความต้องการดังกล่าวได้

แนวทางในการสร้างและนำโมเดลไปใช้งานในปัจจุบัน

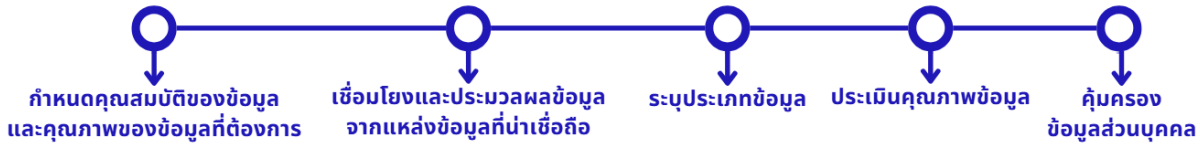
เนื่องจากบริบทในการประยุกต์ใช้ AI และความพร้อมด้านบุคลากรที่แตกต่างกันในแต่ละองค์กร การเลือกใช้เครื่องมือหรือผลิตภัณฑ์ในแต่ละองค์กรจึงมีความแตกต่างกัน โดยบางองค์กรอาจเลือกใช้ผลิตภัณฑ์ AI ที่พร้อมใช้งาน (Off-the-shelf AI Product) หรือว่าจ้างหน่วยงานภายนอกมาดำเนินการทั้งหมด แต่ในขณะที่บางองค์กรอาจมีความต้องการที่จะสร้างและนำโมเดลไปใช้งานด้วยบุคลากรของตนเอง จึงทำให้แนวทางในการสร้างและนำโมเดลไปใช้งานในปัจจุบัน อาจแบ่งออกเป็น 4 แนวทางหลัก

1) **สร้างและนำโมเดลไปใช้ด้วยบุคลากรภายในองค์กร** ดำเนินการตั้งแต่กระบวนการสร้าง สอน ตรวจสอบและทดสอบโมเดล รวมถึงจัดเตรียมข้อมูลสำหรับกระบวนการดังกล่าวด้วยตนเองทั้งหมด ซึ่งแนวทางการสร้างและนำโมเดลไปใช้งานในรูปแบบนี้ จะช่วยให้องค์กรได้ระบบหรือบริการที่ตรงตามความต้องการ แต่จำเป็นต้องลงทุนด้านบุคลากรและเวลามากกว่าแนวทางอื่น
2) **นำโมเดลในรูปแบบโอเพนซอร์ส (Open-source Model) มาปรับใช้** จะช่วยลดเวลาในการสร้างโมเดล แต่อย่างไรก็ตาม องค์กรยังคงมีหน้าที่ในการสอน ตรวจสอบและทดสอบโมเดล รวมถึงจัดเตรียมข้อมูลสำหรับกระบวนการดังกล่าว อีกทั้งยังต้องทำการทดสอบประสิทธิภาพและความสอดคล้องตามข้อกำหนดความต้องการในการการพัฒนาระบบ AI (AI Requirement)
3) **เลือกใช้โมเดลที่ได้รับการสอนแล้ว (Pre-trained Model) มาปรับใช้** จากผู้ให้บริการโซลูชั่นด้าน AI หรือหน่วยงานภายนอกมาปรับใช้นั้น เป็นอีกแนวทางที่ช่วยลดเวลาและภาระในกระบวนการสร้าง สอน ตรวจสอบโมเดล แต่อย่างไรก็ตาม องค์กรยังคงมีหน้าที่ในการจัดเตรียมข้อมูล รวมถึงทดสอบประสิทธิภาพและความสอดคล้องตามข้อกำหนดความต้องการในการการพัฒนาระบบ AI (AI Requirement)
4) **เลือกใช้ผลิตภัณฑ์ AI ที่พร้อมใช้งาน (Off-the-shelf AI Product)** จะช่วยลดเวลาและความซับซ้อนในการพัฒนาระบบ อีกทั้งยังช่วยลดภาระขององค์กรในการสร้างบุคลากรด้าน AI แต่อย่างไรก็ตาม องค์กรยังคงมีความจำเป็นที่จะต้องจัดเตรียมข้อมูลและดำเนินการทดสอบเช่นเดียวกับแนวทางข้างต้น

จากแนวทางการดำเนินการที่ 2 - 4 จะพบว่าองค์กรมีการใช้โมเดลหรือผลิตภัณฑ์ AI ที่สร้างโดยหน่วยงานภายนอก รวมถึงอาจมีการว่าจ้างหน่วยงานภายนอกเพื่อนำโมเดลหรือผลิตภัณฑ์ AI มาปรับใช้ร่วมกับกระบวนการหรือขั้นตอนปฏิบัติต่าง ๆ ให้แก่องค์กร

โดยในกรณีที่มีความเสียหายหรือผลกระทบเชิงลบเกิดความผิดพลาดของหน่วยงานภายนอก รวมถึงความผิดพลาดจากการทำงานของโมเดลหรือผลิตภัณฑ์ AI (ตามแนวทางที่ 2-4) นั้น **องค์กรยังคงต้องรับผิดชอบต่อความเสียหายหรือผลกระทบเชิงลบเช่นเดียวกันกับการดำเนินการตามแนวทางการดำเนินการที่ 1 ด้วยเหตุนี้ องค์กรจึงจำเป็นต้องมีการกำกับดูแลการปฏิบัติงานของหน่วยงานภายนอกให้สอดคล้องตามนโยบายและขั้นตอนปฏิบัติขององค์กร รวมถึงจัดให้มีการทดสอบอย่างเหมาะสม** เพื่อให้มั่นใจได้ว่าโมเดลหรือผลิตภัณฑ์ AI ที่ใช้งานมีประสิทธิภาพและสอดคล้องตามข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement)

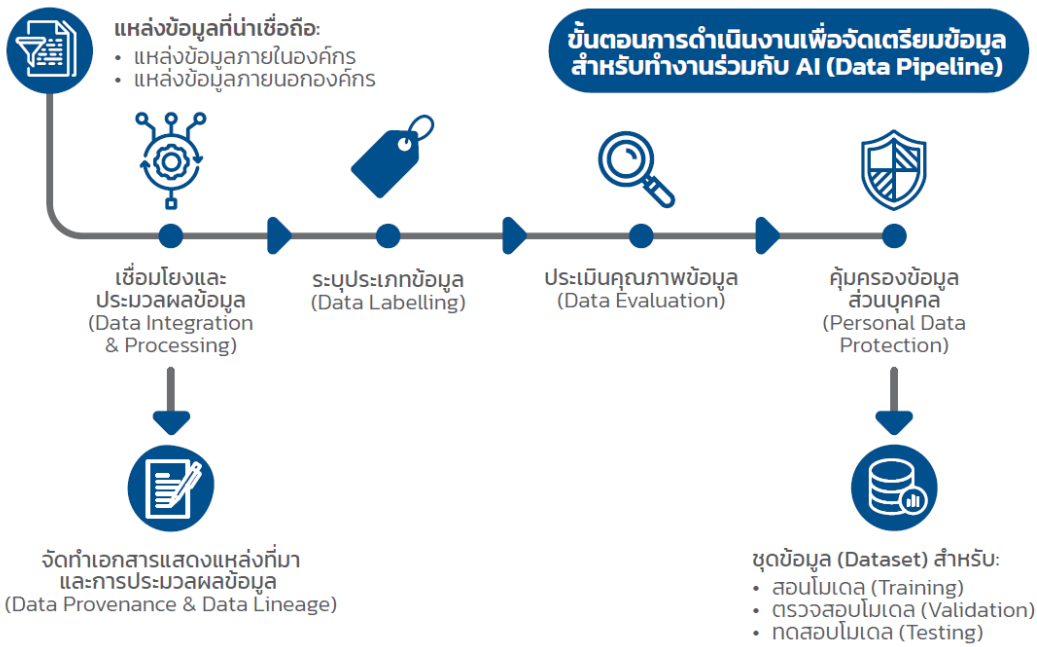
5.1.2 จัดเตรียมข้อมูล (Data Preparation)



เนื่องจาก AI จำเป็นต้องใช้ข้อมูลในการเรียนรู้และประมวลผลในการทำงาน ด้วยเหตุนี้ **องค์กรจึงควรมีการกำหนดคุณสมบัติและคุณภาพของข้อมูลที่เหมาะสม** เพื่อให้ AI สามารถทำงานได้อย่างมีประสิทธิภาพตามเป้าหมายที่กำหนด โดยในการกำหนดคุณสมบัติและคุณภาพนั้น อาจพิจารณาจากประเภทของข้อมูลที่จำเป็นต้องใช้ในการประมวล ขนาดของข้อมูล ความถูกต้องของข้อมูล ข้อมูลมีการจัดเก็บภายในช่วงเวลาที่ต้องการ (Time Series Data) มีการปรับปรุงข้อมูลเป็นประจำสม่ำเสมอ เป็นต้น อีกทั้ง**องค์กรควรมีการสรรหาแหล่งข้อมูลที่น่าเชื่อถือเพื่อนำมาใช้งานร่วมกับ AI**

นอกจากนี้ องค์กรยัง**ควรมีการพิจารณาคุณสมบัติของข้อมูลในด้านอื่นเพื่อลดการเกิดอคติที่มาจากข้อมูล (Data Bias)** เช่น ข้อมูลมีความหลากหลาย ข้อมูลมีความครอบคลุมทุกกลุ่มประชากรโดยไม่เอนเอียงไปยังกลุ่มใดกลุ่มหนึ่ง ขนาดของกลุ่มตัวอย่างสามารถสะท้อนหรือเป็นตัวแทนของประชากรได้อย่างสมเหตุสมผล เป็นต้น **รวมถึงพิจารณาความน่าเชื่อถือของการเก็บรวบรวมข้อมูล เพื่อลดการเกิดอคติที่เกิดจากความคลาดเคลื่อนในการวัดหรือความผิดพลาดจากเครื่องมือวัด (Measurement Bias)**

โดยภายหลังจากทำการเชื่อมโยงเพื่อรวบรวมข้อมูลจากแหล่งต่าง ๆ (Data Integration) เรียบร้อยแล้ว ไม่ว่าจะเป็นแหล่งที่มาจากภายในหรือภายนอกองค์กร **ควรมีการจัดทำเอกสารเพื่อแสดงแหล่งที่มาของข้อมูล (Data Provenance) รวมถึงรายละเอียดการประมวลผลหรือการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อมูลตลอดกระบวนการจัดเตรียมข้อมูล (Data Lineage) เพื่อประโยชน์ในการตรวจสอบย้อนกับ (Traceability)** ในกรณีที่ AI ทำงานผิดพลาด



เนื่องจากในการสร้างโมเดลจำเป็นต้องใช้ข้อมูลในการดำเนินการ โดยเฉพาะอย่างยิ่ง AI ประเภท Supervised Machine Learning จำเป็นต้องเรียนรู้จากข้อมูลที่สอนโดยมนุษย์ เพื่อให้สามารถวิเคราะห์คาดการณ์ให้คำแนะนำ ตัดสินใจ หรือดำเนินการใด ๆ แทนมนุษย์ได้ ด้วยเหตุนี้ **ในการจัดเตรียมข้อมูลสำหรับการสอน ตรวจสอบ และทดสอบโมเดล จำเป็นต้องมีการระบุประเภทของข้อมูล (Data Labelling) อย่างถูกต้อง เพื่อให้ AI มีข้อมูลและสามารถรับรู้ความหมายของข้อมูลได้อย่างถูกต้อง** ซึ่งในการระบุประเภทของข้อมูลสามารถทำได้ทั้งในรูปแบบรูปภาพ ข้อความ และเสียง ตัวอย่างเช่น การระบุรูปคน สัตว์ และสิ่งของต่าง ๆ เพื่อให้ AI สามารถเข้าใจรูปภาพหรือวีดีโอในแบบเดียวกับที่มนุษย์มองเห็น หรือการระบุอารมณ์และความรู้สึกของแต่ละข้อความหรือเสียง เพื่อให้ AI สามารถเข้าใจได้ว่า ผู้ที่แสดงความคิดเห็นดังกล่าวมีความรู้สึกอย่างไร เป็นต้น

โดยก่อนที่จะนำชุดข้อมูล (Dataset) ไปใช้สำหรับการสอน ตรวจสอบ และทดสอบ องค์กรจำเป็นต้องมีการประเมินคุณภาพของข้อมูล (Data Evaluation) และอาจทำการปรับปรุงข้อมูลให้มีคุณภาพตามหลักเกณฑ์ที่องค์กรกำหนด เช่น ข้อมูลมีความถูกต้อง (Accuracy) เนื้อหาข้อมูลครบถ้วน (Completeness) ตรงตามความต้องการ (Relevancy) มีรูปแบบของข้อมูล (Data Format) ตามที่กำหนด และมีการปรับปรุงให้เป็นปัจจุบัน (Timeliness) เป็นต้น **เพื่อให้มั่นใจว่า AI มีความสามารถและประสิทธิภาพเป็นไปตามเป้าหมายที่กำหนด**

นอกจากนี้ ในกรณีที่มีการใช้ข้อมูลส่วนบุคคลในการประมวลผล รวมถึงกรณีที่มีการประมวลผลข้อมูลที่มีความอ่อนไหว (Sensitive Data) ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล องค์กร**ควรมีการเก็บรักษาข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัยและจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม** เช่น การควบคุมการเข้าถึง (Access Control) การเข้ารหัสลับข้อมูล (Encryption) การทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Anonymization) เป็นต้น **เพื่อลดความเสี่ยงที่จะทำให้ข้อมูลส่วนบุคคลรั่วไหล (Data Breach) และป้องกันผลกระทบที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูล**

5.1.3 สร้างโมเดลปัญญาประดิษฐ์ (Model Building)

การสร้างโมเดลนั้นประกอบด้วยขั้นตอนพื้นฐาน 4 ขั้นตอน โดยเริ่มจากการจัดเตรียมอัลกอริทึมสำหรับสร้างโมเดล ซึ่งในขั้นตอนนี้องค์กรอาจพัฒนาอัลกอริทึมขึ้นเองหรืออาจนำอัลกอริทึมที่มีการเปิดเผยซอร์สโค้ด (Open Source) มาใช้งาน โดย**ในกรณีที่องค์กรสร้างโมเดลประเภท Machine Learning นั้น องค์กรจำเป็นต้องทำการสอนโมเดลด้วยชุดข้อมูลสำหรับสอนโมเดล (Training Dataset) จากนั้นจึงนำโมเดลไปตรวจสอบประสิทธิภาพ โดยใช้ชุดข้อมูลสำหรับตรวจสอบโมเดล (Validation Dataset)** ซึ่งหาก AI ยังไม่สามารถทำงานได้ตามประสิทธิภาพที่กำหนด **โมเดลดังกล่าวจะถูกปรับแต่ง (Tuning) และนำกลับไปตรวจสอบจนกว่าประสิทธิภาพในการทำงานจะเป็นไปตามเป้าหมายที่กำหนด โดยโมเดลที่ดีที่สุดจะถูกนำไปทดสอบด้วยชุดข้อมูลสำหรับทดสอบโมเดล (Testing Dataset) ในขั้นตอนสุดท้ายก่อนนำไปใช้งาน (Deployment)** ซึ่งชุดข้อมูลสำหรับทดสอบโมเดลนี้จะต้องเป็นชุดข้อมูลที่ไม่เคยถูกใช้ในขั้นตอนการสอนและตรวจสอบโมเดลมาก่อน

สำหรับองค์กรที่เลือกใช้โมเดลจากผู้ให้บริการโซลูชั่นด้าน AI (AI Solution Provider) ถึงแม้ว่าองค์กรจะไม่จำเป็นต้องทำการสร้างโมเดลด้วยตนเอง แต่องค์กรยังคงมีหน้าที่ในการทดสอบว่าโมเดลสามารถทำงานได้อย่างมีประสิทธิภาพและสามารถบรรลุตามเป้าหมายที่กำหนด พร้อมทั้ง มีหน้าที่ในการ**พิจารณาและตรวจสอบความเหมาะสมของกระบวนการสร้างโมเดล** เช่น ขั้นตอนและข้อมูลที่เกี่ยวข้องกับกระบวนการสร้าง สอน และทดสอบโมเดล รวมถึงมาตรการต่าง ๆ ที่เกี่ยวข้อง เป็นต้น

นอกเหนือจากการควบคุมกระบวนการสร้างโมเดลข้างต้นเพื่อให้ AI มีประสิทธิภาพและสามารถบรรลุเป้าหมายตามที่กำหนด **องค์กรยังจำเป็นต้องจัดให้มีมาตรการควบคุมเพื่อให้มั่นใจได้ว่า การทำงานของ AI สอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ รวมถึงกฎหมายและข้อกำหนดที่เกี่ยวข้อง**

โดยในการพิจารณาว่าการทำงานของ AI ควรสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ใดนั้น **องค์กรควรพิจารณาจากบริบทของการนำ AI ไปประยุกต์ใช้ ความเสี่ยง และผลกระทบที่อาจเกิดขึ้น โดยไม่จำเป็นต้องดำเนินการให้สอดคล้องกับทุกหลักการจริยธรรมปัญญาประดิษฐ์ที่กล่าวถึงในเอกสารนี้**

- **ความน่าเชื่อถือ (Reliability)**

  เพื่อให้การทำงานของ AI มีความน่าเชื่อถือ องค์กรควรมีการกำหนดมาตรการและควบคุมกระบวนการสร้างและทดสอบโมเดล เพื่อให้มั่นใจได้ว่า**โมเดลสามารถสร้างผลลัพธ์ได้เหมือนเดิมทุกครั้ง (Reproducibility) เมื่ออยู่ภายใต้สถานการณ์หรือได้รับข้อมูลที่เหมือนกัน อีกทั้งยังสามารถทนทาน (Robustness) ต่อเหตุการณ์ที่อาจเกิดความผิดพลาดหรือสร้างผลกระทบเชิงลบได้**

  โดยในการทดสอบความทนทานต่อเหตุการณ์ที่อาจเกิดความผิดพลาดหรือสร้างผลกระทบเชิงลบนั้น องค์กรจำเป็นต้องทำการทดสอบโดยใช้ข้อมูลที่อยู่นอกเหนือจากขอบเขตที่ออกแบบไว้ (Exceptions) รวมถึงทำการทดสอบภายใต้สถานการณ์หรือข้อมูลที่ได้เคยถูกสอนมาก่อน เพื่อให้มั่นใจว่า AI ยังคงสามารถทำงานได้อย่างถูกต้องตามที่ออกแบบไว้หรือสามารถรับมือกับเหตุการณ์ที่เกิดขึ้นโดยไม่ส่งผลกระทบเชิงลบต่อบุคคล องค์กรและสังคมโดยกว้าง

  นอกจากนี้ในการทดสอบความทนทาน องค์กรยังจำเป็นต้องเฝ้าติดตามและนำผลลัพธ์การทำงานของ AI มาปรับปรุงอย่างต่อเนื่อง เพื่อให้ AI สามารถทำงานได้อย่างมีประสิทธิภาพภายใต้สภาพแวดล้อมการใช้งานจริงและอยู่ในขอบเขตที่ยอมรับได้

- **ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)**

  ผลลัพธ์จากการทำงานของ AI ไม่ว่าอยู่ในรูปแบบของการวิเคราะห์คาดการณ์ การให้คำแนะนำ การตัดสินใจ หรือการดำเนินการใด ๆ นั้น อาจส่งผลกระทบให้เกิดความไม่เป็นธรรม (Unfairness) จนนำไปสู่การเลือกปฏิบัติ (Discrimination) ซึ่งผลกระทบดังกล่าวนั้นอาจเกิดจากอคติที่มาจากข้อมูล (Data Bias) หรืออคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced By Engineering Decisions)

  เพื่อป้องกันความไม่เป็นธรรมซึ่งเกิดจากอคติที่มาจากการออกแบบและสร้างโมเดล (Bias Introduced By Engineering Decisions) นั้น **บุคลากรที่เกี่ยวข้องกับกระบวนการสร้างและการทดสอบโมเดลจึงควรมีความรู้และมีความหลากหลาย รวมถึงจัดให้มีผู้เชี่ยวชาญในด้านที่เกี่ยวข้องกับการประยุกต์ใช้ AI คอยให้คำปรึกษา** เพื่อให้องค์กรมองเห็นอคติที่อาจเกิดขึ้นและกำหนดกลยุทธ์ในการลดอคติดังกล่าว

สำหรับ**อคติที่มาจากข้อมูล (Data Bias) นั้น อาจเกิดจากการมีข้อมูลที่เอนเอียงไม่ครอบคลุมทุกกลุ่มประชากร หรือมีขนาดของกลุ่มตัวอย่างที่ไม่เหมาะสม ทำให้เกิดความไม่เป็นธรรม (ซึ่งเรียกว่า “Selection Bias”)** อีกทั้งในบางกรณีอาจเกิดจากอคติที่มาจากความคลาดเคลื่อนในการวัดหรือความผิดพลาดจากเครื่องมือวัด (Measurement Bias)

องค์กรอาจพิจารณาเลือกใช้มาตรการดังต่อไปนี้ เพื่อลดอคติที่มีจากข้อมูล ตัวอย่างเช่น

1. เลือกใช้ข้อมูลจากแหล่งข้อมูลที่มีความน่าเชื่อถือและมีการเก็บรวบรวมข้อมูลอย่างถูกต้อง
2. ข้อมูลมีความหลากหลายและครอบคลุมทุกกลุ่มประชากร อีกทั้งมีการรวบรวมมาจากแหล่งข้อมูลที่หลากหลาย (หากเป็นไม่ได้)
3. ขนาดของกลุ่มตัวอย่างสามารถสะท้อนหรือเป็นตัวแทนของประชากรได้อย่างสมเหตุสมผล
4. ระมัดระวังในการเลือกใช้ข้อมูลเฉพาะกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง รวมถึงข้อมูลที่มีความอ่อนไหว (Sensitive Data) ตัวอย่างเช่น เพศ เชื้อชาติ ศาสนา ประวัติการรักษาพยาบาล ประวัติอาชญากรรม เป็นต้น
5. พิจารณากำหนดชุดข้อมูลสำหรับทดสอบแต่ละชุดให้มีความแตกต่างกันของกลุ่มประชากร เพื่อตรวจสอบว่า AI ยังคงตัดสินใจได้อย่างถูกต้อง ไม่เอนเอียงไปตามกลุ่มประชากรกลุ่มใดกลุ่มหนึ่ง
6. อาจพิจารณาสุ่มข้อมูลที่คาดว่าจะส่งผลให้เกิดอคติ เพื่อค้นหาความผิดพลาด พร้อมทั้งเก็บรวบรวมข้อมูลดังกล่าวสำหรับใช้ในครั้งต่อไป

- **ความโปร่งใส (Transparency)**

ความสามารถในการอธิบายรายละเอียดเกี่ยวกับ AI (Explainability) เป็นหนึ่งในมาตรการสำคัญที่จะช่วยให้เกิดความโปร่งใสในการประยุกต์ใช้งาน AI โดย**องค์กรจำเป็นต้องมีการจัดทำเอกสารเพื่ออธิบายพฤติกรรมการทำงานของ AI และเหตุผลเบื้องหลังการทำงาน รวมถึงอธิบายกระบวนการในการสร้างและทดสอบโมเดล** ซึ่งจะช่วยให้ผู้ที่เกี่ยวข้องรับทราบและเข้าใจถึงกระบวนการทำงานของ AI อีกทั้งยังเป็นการสร้างความเชื่อมั่นและการยอมรับจากบุคคลที่เกี่ยวข้องอีกด้วย

นอกจากนี้ เพื่อให้เกิดความโปร่งใสในการประยุกต์ใช้ AI **องค์กรควรมีการดำเนินการเพื่อให้สามารถตรวจสอบย้อนกลับ (Traceability)** ในกรณีที่พบความผิดปกติหรือความผิดพลาดได้ **โดยทำการเก็บรวบรวมข้อมูลและรายละเอียดที่เกี่ยวข้องกับกระบวนการในการสร้างและทดสอบโมเดล** เช่น

- แหล่งที่มาของข้อมูล (Data Provenance)
- การประมวลผลหรือการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อมูลตลอดกระบวนการจัดเตรียมข้อมูล (Data Lineage)
- รายละเอียดการออกแบบและการทำงานของอัลกอริทึม
- ชุดข้อมูลที่ใช้และผลลัพธ์ในการสอน ตรวจสอบ และทดสอบโมเดล
- ผลการประเมินความเสี่ยงและมาตรการการรับมือ

- **ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)**

ในด้านการรักษาความมั่นคงปลอดภัยและการคุ้มครองความเป็นส่วนตัวนั้น การปฏิบัติตามแนวปฏิบัติที่ดีในการพัฒนาซอฟต์แวร์ (เช่น การควบคุมเวอร์ชัน การทดสอบ และควบคุมคุณภาพ

ของซอร์สโค้ด เป็นต้น) อาจจะไม่เพียงพอต่อการรักษาความมั่นคงปลอดภัยและคุ้มครองความเป็นส่วนตัว เนื่องจาก **AI อาจมีช่องโหว่ที่เปิดโอกาสให้ผู้ประสงค์ร้ายโจมตีข้อมูลที่ใช้ในการสอนโมเดลและโจมตีที่โมเดลโดยตรง** ตัวอย่างเช่น

- Poisoning Attack เป็นการโจมตีโดยทำให้ข้อมูลที่ในสอนโมเดลปนเปื้อนด้วยข้อมูลที่ทำให้โมเดลเกิดช่องโหว่ (Adversarial Manipulation) เพื่อให้ผู้ประสงค์ร้าย (Attacker) สามารถบรรลุเป้าหมายที่ต้องการ
- Evasion Attack เป็นการโจมตีโมเดลโดยตรง โดยส่งข้อมูลที่ทำให้โมเดลประมวลผลแล้วทำงานผิดพลาดหรือหยุดการทำงาน (Adversarial Input)

เพื่อป้องกันภัยคุกคามข้างต้นจึงจำเป็นต้องมีความร่วมมือกันระหว่างนักพัฒนา AI (AI Developer) นักวิทยาศาสตร์ข้อมูล (Data Scientist) นักวิเคราะห์ข้อมูล (Data Analyst) ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย รวมถึงผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ในการจัดทำมาตรฐานเพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้น โดยปฏิบัติตามมาตรฐานหรือแนวทางการรักษาความมั่นคงปลอดภัย นอกจากนี้ควรติดตามข่าวสารเกี่ยวกับภัยคุกคามจากแหล่งข้อมูลต่าง ๆ เช่น The open Worldwide Application Security Project (OWASP)

นอกจากนี้ ในการคุ้มครองความเป็นส่วนตัว **ควรมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) รวมถึงจัดให้มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม** ซึ่งได้กล่าวมาแล้วในหัวข้อการจัดเตรียมข้อมูล (Data Preparation)

5.1.4 นำโมเดลไปใช้งาน (Deployment)

ก่อนนำโมเดลไปใช้งานจริง **องค์กรควรมีการนำโมเดลไปติดตั้งและทดสอบการทำงานภายใต้สภาพแวดล้อมเสมือนจริง (Pre-Production Environment) เพื่อทดสอบการทำงานร่วมกับขั้นตอนปฏิบัติงานที่เกี่ยวข้อง พร้อมทั้งทดสอบความสามารถในการรองรับปริมาณการใช้งาน (Workload) และความสามารถในการตอบสนองภายในระยะเวลาที่ยอมรับได้ (Acceptable Latency Time)** ซึ่งการติดตั้งและทดสอบในสภาพแวดล้อมดังกล่าว จะช่วยให้องค์กรพบปัญหาและสามารถป้องกันปัญหาที่อาจเกิดขึ้นก่อนนำโมเดลไปใช้งานจริง อีกทั้งยังเป็นการสร้างความน่าเชื่อถือ (Reliability) ให้แก่ระบบหรือบริการ

นอกจากนี้ ก่อนนำโมเดลไปใช้งานจริงองค์กรควรมีการ**ออกแบบสถาปัตยกรรมที่เกี่ยวข้องกับการประยุกต์ใช้ AI (AI Architecture) ที่มีประสิทธิภาพและสามารถรองรับปริมาณการใช้งานได้อย่างเพียงพอ เพื่อให้การประยุกต์ใช้ AI บรรลุตามเป้าหมายที่กำหนด พร้อมทั้งอาจพิจารณาออกแบบสถาปัตยกรรมให้มีความยืดหยุ่น**เพื่อรองรับความต้องการเพิ่มขึ้นหรือการขยายขอบเขตการใช้งานในอนาคตได้

เพื่อให้องค์กรมีความพร้อมในการทำงานหรือให้บริการอย่างต่อเนื่อง องค์กรจึงควรมี**การบริหารจัดการความเปลี่ยนแปลง (Change Management) เพื่อลดผลกระทบที่อาจเกิดขึ้นจากการนำโมเดลไปใช้งานร่วมกับขั้นตอนปฏิบัติงานจริง** นอกจากนี้ ในการบริหารจัดการความเปลี่ยนแปลงดังกล่าว ยังจำเป็นต้องครอบคลุม

ถึงกรณีที่มีการปรับปรุงแก้ไขโมเดลและการยุติการใช้งานโมเดลด้วยเช่นกัน เพื่อไม่ให้การเปลี่ยนแปลงใด ๆ ที่เกี่ยวข้องกับโมเดลส่งผลกระทบต่อการทำงานหรือการให้บริการ

เนื่องจาก AI เป็นเทคโนโลยีสารสนเทศประเภทหนึ่งที่ต้องทำงานร่วมกับระบบเทคโนโลยีสารสนเทศที่หลากหลาย เช่น ระบบปฏิบัติการ (Operating System) ระบบเครือข่าย (Network System) ระบบบริหารคลาวด์ (Cloud Computing) ระบบบริหารจัดการข้อมูล (Data Management System) เป็นต้น ดังนั้น ผลกระทบใด ๆ ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศดังกล่าวย่อมส่งผลกระทบต่อการทำงานของ AI ด้วยเช่นกัน ด้วยเหตุนี้ **องค์กรจึงควรมีมาตรกรในการรักษาความมั่นคงปลอดภัยสารสนเทศและคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้ และป้องกันผลร้ายที่อาจเกิดขึ้น** เช่น การโจรกรรมข้อมูลสำคัญขององค์กร ข้อมูลส่วนบุคคลรั่วไหล การโจมตีช่องโหว่ของโมเดลเพื่อให้ระบบบริการหยุดชะงักหรือใช้ประโยชน์จากความผิดพลาดเพื่อเข้าถึงระบบ เป็นต้น

นอกจากนี้ เพื่อให้องค์กรสามารถรับมือกับเหตุการณ์ผิดปกติและลดผลกระทบที่อาจเกิดขึ้นได้อย่างทันท่วงที องค์กรจึงควร**จัดให้มีช่องทางรับข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) ความผิดพลาด (Error) จากการปฏิบัติงานและการให้บริการ พร้อมทั้งจัดให้มีมาตรการในการบริหารจัดการเหตุกาณ์ผิดปกติ (Incident Management) เพื่อรับมือและแก้ไขปัญหาที่เกิดขึ้น** อีกทั้งยังเป็นการลดผลกระทบที่อาจเกิดขึ้นต่อบุคคลองค์กร หรือสังคมโดยกว้าง

5.1.5 เฝ้าติดตามการประยุกต์ใช้ (Monitoring)

ภายหลังจากนำโมเดลไปใช้งานในระบบบริการจริง องค์กร**ควรมีการเฝ้าติดตามประสิทธิภาพ (Performance) ของการประยุกต์ใช้ AI ในด้านความสำเร็จตามเป้าหมายและประสิทธิภาพในการทำงานของ AI พร้อมทั้งปรับแต่งค่า (Model Tuning) เมื่อมีความจำเป็น** เพื่อให้มั่นใจได้ว่าโมเดลยังสามารถทำงานได้ตามเป้าหมายที่องค์กรกำหนด พร้อมทั้งจัดให้มีกระบวนการใน**การเฝ้าติดตามว่ามีข้อมูลใหม่ที่ควรนำมาใช้ในการสอนโมเดลเพื่อปรับปรุงประสิทธิภาพของ AI** หรือไม่ นอกจากนี้ การเฝ้าติดตามยัง**รวมถึงการปฏิบัติงานตามนโยบายขององค์กร หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้องอย่างสม่ำเสมอ**

โดยในการเฝ้าติดตามประสิทธิภาพของการประยุกต์ใช้ AI นั้น อาจดำเนินการโดยพิจารณาจากผลลัพธ์จากการทำงาน ระดับความถูกต้องในการตัดสินใจ (Accuracy Rate) ข้อคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาดที่เกิดขึ้น (Error) เป็นต้น ทั้งนี้หากองค์กรมีเครื่องมือที่ช่วยในการเฝ้าติดตามและมีการรายงานผลโดยอัตโนมัติ ไม่ว่าจะอยู่ในรูปแบบของการรายงานผ่านหน้าจอสรุปข้อมูล (Dashboard) หรือมีการแจ้งเตือนผ่านช่องทางต่าง ๆ จะช่วยเพิ่มประสิทธิภาพในการเฝ้าติดตาม อีกทั้งยังช่วยลดภาระในการเฝ้าติดตามและรายงานผลคณะกรรมการกำกับดูแลฯ เพื่อรับทราบ

5.1.6 ประเมินผลการประยุกต์ใช้ (Evaluation)

การประเมินผลการประยุกต์ใช้ AI **เป็นการนำผลลัพธ์จากการประยุกต์ใช้ในปัจจุบันมาพิจารณาเพื่อกำหนดแนวทางการดำเนินการในอนาคต** โดยอาจพิจารณาในด้านต่าง ๆ เช่น

- ประสิทธิภาพ (Performance) ของการประยุกต์ใช้ AI ในด้านความสำเร็จตามเป้าหมายและประสิทธิภาพในการทำงานของ AI ที่ผ่านมา เมื่อเทียบกับเป้าหมายที่กำหนดความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง

- พิจารณาปรับปรุงเป้าหมายในการประยุกต์ใช้ AI หากพบว่าการประยุกต์ใช้ AI ไม่สามารถช่วยให้องค์กรบรรลุตามเป้าหมายที่กำหนดได้ หรือมีเหตุจำเป็นที่ต้องปรับปรุงเป้าหมาย
- ปรับปรุงข้อกำหนดความต้องการในการพัฒนาระบบ AI (AI Requirement) หากพบว่าข้อกำหนดความต้องการไม่ถูกต้อง หรือยกเลิกข้อกำหนดในบางเรื่องหากพบว่าไม่มีความจำเป็น
- วิเคราะห์และทบทวนความเสี่ยงจากการดำเนินงานที่ผ่านมา รวมถึงวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นในอนาคต เพื่อปรับปรุงแผนการจัดการความเสี่ยง (Risk Treatment Plan) ให้เหมาะสม

โดยการในการประเมินผลการประยุกต์ใช้ AI นั้น **อาจจัดให้มีการประเมินผลโดยผู้ตรวจประเมินภายใน (Internal Auditor) หรือผู้ตรวจประเมินภายนอก (External Auditor) ตามความเหมาะสมเพื่อช่วยเพิ่มความน่าเชื่อถือ (Reliability)** ให้แก่บริการ พร้อมทั้งแจ้งผลการตรวจประเมินให้คณะกรรมการกำกับดูแลฯ รับทราบ เพื่อพิจารณาและกำหนดแนวทางการดำเนินงานในอนาคต รวมถึงสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องรับทราบและดำเนินการตามแนวทางที่กำหนด

5.1.7 ยุติการใช้งาน (Retirement)

ในกรณีที่โมเดล ผลิตภัณฑ์ ระบบหรือบริการที่เกี่ยวข้องกับ AI **ไม่สามารถช่วยให้องค์กรบรรลุตามเป้าหมายหรือตอบโจทย์ความต้องการทางธุรกิจได้อย่างมีประสิทธิภาพ ซึ่งอาจเกิดจากเทคโนโลยีที่ใช้นั้นล้าสมัย (Obsolete) หรือผลลัพธ์จากการทำงานของ AI ในปัจจุบันไม่สามารถตอบสนองต่อความต้องการขององค์กรที่เปลี่ยนแปลงได้** ซึ่งในกรณีดังกล่าวองค์กรอาจพิจารณาดำเนินการใน 2 กรณี กล่าวคือ

1. ยุติการใช้งานโมเดล ระบบ หรือบริการที่เกี่ยวข้องกับ AI ดังกล่าว
2. นำโมเดล ผลิตภัณฑ์ ระบบหรือบริการที่เกี่ยวข้องกับ AI ใหม่ มาใช้งานทดแทนของเดิม (Replace) หากองค์กรพบว่ามีแนวทางใหม่ที่มีประสิทธิภาพดีกว่า หรือสามารถตอบสนองต่อความต้องการขององค์กรที่เปลี่ยนแปลงไปได้

5.2 การให้บริการ AI (AI Service)

การสื่อสารเพื่อสร้างความสัมพันธ์ระหว่างองค์กรและผู้ใช้งานนั้น มีความสำคัญอย่างยิ่งต่อการสร้างความโปร่งใสในการให้บริการ อีกทั้งยังเป็นการสร้างความเชื่อมั่นของผู้ใช้งานที่มีต่อบริการและองค์กร ด้วยเหตุนี้ **องค์กรจึงควรมีการสื่อสารนโยบายในการให้บริการ ข้อกำหนดในการให้บริการ และข้อมูลที่เกี่ยวข้องกับการใช้งาน AI รวมถึงการเปิดให้มีช่องทางการติดต่อสื่อสารกับผู้ใช้งานเพื่อรับฟังเสียงสะท้อนจากการใช้งานจริง** ดังตัวอย่างต่อไปนี้

- **การประกาศนโยบายและข้อมูลทั่วไปเกี่ยวกับการใช้งาน AI (Policy and General Disclosure)**

  ในการให้บริการที่เกี่ยวข้องกับ AI องค์กรควรมีการแจ้งให้ผู้ใช้งานรับทราบถึงนโยบายด้านต่าง ๆ เกี่ยวกับการให้บริการ ตัวอย่างเช่น นโยบายในการใช้งาน AI (AI Usage Policy) แนวปฏิบัติตามหลักจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) นโยบายด้านความมั่นคงปลอดภัย (Security Policy) นโยบายความเป็นส่วนตัว (Privacy Policy) เป็นต้น

  นอกจากนี้ องค์กรยัง**ควรมีการแจ้งผู้ใช้งานทราบว่ากำลังใช้งาน รับบริการ หรือทำงานร่วมกับ AI ผ่านการแจ้งเตือนบนแอปพลิเคชัน (In-app Notification)** พร้อมทั้งควรมีการแจ้งถึงวิธีการใช้งาน

ข้อห้ามในการใช้งาน ความสามารถ ข้อจำกัด ผลลัพธ์จากการตัดสินใจของ AI รวมถึงวิธีการและเหตุผลเบื้องหลังการทำงานของ AI ผ่านทางคู่มือการใช้งาน คำถามที่พบบ่อย (FAQ) และข้อตกลงการใช้บริการ (Terms and Conditions) เป็นต้น

- **การปิดการทำงานของ AI (AI Function Opt-out)**

  ในกรณีที่ระบบสามารถเปิดโอกาสให้ผู้ใช้งานปิดการทำงานของ AI ได้ด้วยตนเอง เช่น รถยนต์ที่มีระบบการขับเคลื่อนอัตโนมัติด้วยตนเอง อนุญาตให้ผู้ใช้งานสามารถปิดระบบขับเคลื่อนอัตโนมัติด้วยตนเองได้ เป็นต้น องค์กรควรมีการสื่อสารอย่างเหมาะสมเพื่อให้ผู้ใช้งานทราบถึงขั้นตอนการปิดการทำงานดังกล่าว

- **ช่องทางการติดต่อสื่อสาร (Communication Channel)**

  การเปิดช่องทางการติดต่อสื่อสารเพื่อเปิดรับความคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) ที่พบโดยผู้ใช้งานนั้นมีความสำคัญมาก เนื่องจากจะช่วยให้องค์กรสามารถปรับปรุง รวมถึงแก้ไขปัญหาและความผิดพลาดที่พบจากการให้บริการจริง อีกทั้งยังช่วยในการปรับปรุงประสบการณ์ในการให้บริการและป้องกันปัญหาหรือผลกระทบที่อาจเกิดขึ้นในอนาคต

6 การประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาล

6.1 ทำความเข้าใจ Generative AI

6.1.1 ความหมายของ Generative AI

Generative AI เป็น AI ประเภทหนึ่งที่**สามารถสร้างเนื้อหาได้หลากหลายรูปแบบ** เช่น ข้อความ ภาพ วิดีโอ ซอร์สโค้ด หรือรูปแบบอื่น เป็นต้น **ด้วยการสั่งการผ่านข้อความหรือคำสั่ง (Prompt)** ที่มนุษย์เป็นผู้กำหนด

เมื่อ Generative AI ได้รับ Prompt จากผู้ใช้งานแล้ว **Generative AI จะทำการสร้างเนื้อหาใหม่ที่คล้ายคลึงกับข้อมูลที่ได้รับการฝึกฝนมา** โดยเลือกนำเสนอเนื้อหาที่สอดคล้องและเหมาะสมกับ Prompt ที่ได้รับมามากที่สุด **โดยพิจารณาจากหลักการความน่าจะเป็น** เช่น ChatGPT, Gemini, Canva และ อื่น ๆ

จากความสามารถและกระบวนการทำงานของ Generative AI ข้างต้น จึงทำให้ Generative AI มีความแตกต่างจาก AI แบบเดิม (Traditional AI) กล่าวคือ Traditional AI ถูกออกแบบมาเพื่อคาดการณ์ (Prediction) การตัดสินใจ (Decision) หรือการให้คำแนะนำ (Recommendation) บนพื้นฐานของข้อมูลที่ได้รับการฝึกฝน (Train) มาก่อน ตัวอย่างเช่น การใช้ AI แนะนำสินค้าและบริการ เป็นต้น แต่ AI แบบนี้ไม่ได้ถูกออกแบบมาเพื่อสร้างเนื้อหาใหม่ที่มีความคล้ายคลึงกับข้อมูลต้นฉบับ

จากรูปที่แสดงลำดับถัดไปจะพบว่า Generative AI เป็น AI ประเภทหนึ่งของ Deep Learning เนื่องจาก Generative AI สร้างเนื้อหาใหม่บนพื้นฐานของข้อมูลที่ได้รับการฝึกฝนมา โดยทำการประมวลผลเพื่อสร้างเนื้อหาใหม่ผ่านโครงข่ายประสาทเทียม (Artificial Neural Network) ที่มีความซับซ้อน

6.2 ประโยชน์และข้อจำกัดของ Generative AI

6.2.1 ประโยชน์จากการประยุกต์ใช้ Generative AI

Generative AI มีความสามารถที่โดดเด่นในการสร้างสรรค์สิ่งใหม่ ช่วยเพิ่มประสิทธิภาพกระบวนงานภายในองค์กร ดังนั้น องค์กรจึงควรเริ่มจากการทำความเข้าใจศักยภาพของเทคโนโลยีนี้ เพื่อให้สามารถนำไปประยุกต์ใช้ให้เกิดประโยชน์อย่างเหมาะสม

- สร้างสรรค์ไอเดีย และร่างเนื้อหาใหม่ (Ideation and Content Creation)
- สืบค้นและเข้าถึงข้อมูล (Information Discovery and Accessibility)
- สรุปความและเรียบเรียงเนื้อหาใหม่ (Content Refinement)
- วิเคราะห์ข้อมูลและให้ข้อเสนอแนะ (Data Analysis and Recommendations)
- สร้างและปรับปรุงซอร์สโค้ด (Source Code Generation and Optimization)
- สร้างและปรับปรุงมัลติมีเดีย (Multimedia Creation and Editing)

6.2.2 ข้อจำกัดของ Generative AI

เพื่อให้องค์กรสามารถเลือกนำ Generative AI ไปประยุกต์ใช้งานได้อย่างเหมาะสมจึงควรเข้าใจข้อจำกัดของเทคโนโลยีนี้ พร้อมทั้งประเมินความเหมาะสมในการประยุกต์ใช้ และวางแผนรับมือกับข้อจำกัดที่อาจเกิดขึ้น

- **อาการหลอน (Hallucination หรือ Confabulation):** Generative AI สามารถสร้างคำตอบที่ดูเหมือนมีเหตุผลแต่ไม่ถูกต้องตามข้อเท็จจริง เช่น ผู้ใช้งานได้ใช้ Generative AI เพื่อขอรับคำแนะนำการลงทุนในหุ้นตามเงื่อนไขที่ต้องการ ซึ่งได้ผลลัพธ์ออกมาน่าเชื่อถือมาก แต่กลับพบว่าคำแนะนำของ Generative AI นั้น เป็นการเสนอให้ลงทุนในหุ้นบริษัทที่ไม่มีอยู่จริง
- **การคิดวิเคราะห์และการตัดสินใจ (Critical Thinking and Judgement):** เนื่องจาก Generative AI ประมวลผลเพื่อสร้างข้อความโดยใช้หลักการความน่าจะเป็นของคำถัดไป จึงอาจทำให้ได้ข้อสรุปที่ไม่ถูกต้องหรือไม่สมเหตุสมผล เช่น เจ้าหน้าที่การตลาดขอคำแนะนำจาก Generative AI เพื่อวางแผนการตลาดเครื่องดื่มสุขภาพ Generative AI แนะนำให้ใช้กลยุทธ์การแจกผลิตภัณฑ์ฟรีในโรงเรียนเพราะว่าพบว่ากลยุทธ์นี้ประสบความสำเร็จในอุตสาหกรรมอื่น แต่ก็ไม่ได้คำนึงถึงว่ากลุ่มเป้าหมายของบริษัทรวมถึงผู้สูงอายุ คนทำงาน
- **บริบทที่ละเอียดอ่อน หรือประเด็นทางจริยธรรม (Sensitive or Ethical Context):** Generative AI สามารถสร้างเนื้อหาที่ไม่เหมาะสมตามหลักจริยธรรม มีความเอนเอียง หรือเนื้อหาที่นำไปสู่การเลือกปฏิบัติ เช่น ผู้ใช้งานขอคำแนะนำจาก Generative AI เกี่ยวกับการเลือกอาชีพ โดยได้รับคำแนะนำให้เพศชายเลือกอาชีพวิศวกร และให้ข้อมูลว่ามีค่าตอบแทนสูง ขณะที่แนะนำให้เพศหญิงเลือกอาชีพพยาบาลและให้ข้อมูลว่ามีความเหมาะสมดีแล้ว
- **ความเชี่ยวชาญเฉพาะด้าน (Domain Expertise):** ผลลัพธ์ของ Generative AI ไม่สามารถใช้แทนข้อแนะนำหรือข้อคิดเห็นจากผู้เชี่ยวชาญได้ โดยเฉพาะในด้านกฎหมาย การแพทย์ หรือด้านอื่น ๆ ที่ต้องการข้อมูลที่ถูกต้องแม่นยำ เช่น ผู้ป่วยรายหนึ่งขอคำแนะนำการรักษาจาก Generative AI สำหรับอาการปวดท้อง ซึ่ง Generative AI แนะนำให้ใช้ยาลดกรดเพราะเป็นวิธีที่ได้ผลในอาการ

คล้ายกับที่ผู้ป่วยสอบถาม แต่ในความเป็นจริง ผู้ป่วยรายนี้มีปัญหาเกี่ยวกับตับอ่อน การใช้ยาลดกรดจึงไม่เหมาะสมและอาจทำให้อาการแย่ลง

- **ประสบการณ์และบริบทเฉพาะบุคคล (Personal Experience and Context):** ถึงแม้ผลลัพธ์จาก Generative AI อาจดูเหมือนสร้างมาจากมนุษย์แต่แท้จริง Generative AI ยังขาดการมีประสบการณ์และอารมณ์ความรู้สึกเหมือนมนุษย์ เช่น ผู้ใช้งานขอคำแนะนำจาก Generative AI เกี่ยวกับการศึกษาต่อ โดย Generative AI แนะนำให้ผู้ใช้งานศึกษาวิศวกรรมศาสตร์เพราะมีโอกาสในการทำงานและค่าตอบแทนสูง แต่ผู้ใช้งานมีความสนใจและความสามารถทางด้านศิลปะและออกแบบ คำแนะนำนี้จึงไม่สอดคล้องกับความสนใจและความสามารถของผู้ใช้งาน
- **ความเป็นปัจจุบันของข้อมูล (Dynamic Real-time Information Retrieval):** ข้อมูลผลลัพธ์จาก Generative AI อาจยังไม่รวมข้อมูลจากอินเทอร์เน็ต หรือไม่สามารถเข้าถึงข้อมูลที่อยู่นอกชุดข้อมูลที่ใช้ในการฝึกฝนโมเดลแบบ Real-Time เช่น ผู้ใช้งานขอคำแนะนำจาก Generative AI เกี่ยวกับข้อมูลด้านกฎหมาย ซึ่งได้รับคำตอบที่น่าเชื่อถือแต่เป็นข้อมูลที่ไม่เป็นปัจจุบันจากอินเทอร์เน็ต เช่น กฎหมายที่ไม่มีผลบังคับใช้อีกต่อไป ทำให้คำแนะนำที่ได้รับไม่ถูกต้องตามสถานการณ์ปัจจุบัน
  หมายเหตุ: ในปัจจุบันผลิตภัณฑ์ LLM ต่าง ๆ เช่น ChatGPT Gemini และ Bing ได้มีการปรับให้ผลลัพธ์ที่แสดงรายการเข้าถึงข้อมูลจากอินเทอร์เน็ตแล้ว
- **การให้เหตุผลเกี่ยวกับผลลัพธ์ (Explainability):** การอธิบายกระบวนการทำงานภายในโมเดล Generative AI เป็นเรื่องยาก เนื่องจากโมเดลขึ้นอยู่กับโครงข่ายประสาทเทียม (Neural Network) ที่เรียกว่า Black Box ซึ่งอาจส่งผลกระทบหากต้องมีการชี้แจงเหตุผลของผลลัพธ์ที่ได้มาจากโมเดล
- **ความไม่แน่นอนของผลลัพธ์ (Consistent Output):** ผลลัพธ์ของ Generative AI ไม่คงที่ แม้ว่าจะป้อนข้อมูลเข้าไปแบบเดียวกัน แต่อาจได้คำตอบที่ต่างกัน เช่น บริษัทใช้ Generative AI เพื่อตอบคำถามผู้สนใจสมัครงาน สำหรับตำแหน่งเดียวกัน โดย Generative AI ให้คำอธิบายที่แตกต่างกันแก่ผู้สมัครหลายคน ทั้งที่เป็นตำแหน่งงานเดียวกัน ทำให้ผู้สมัครเกิดความสับสน เข้าใจลักษณะงานที่ไม่ถูกต้อง

จากข้อจำกัดในการนำ Generative AI มาประยุกต์ใช้ข้างต้น องค์กรจึงควรคำนึงถึงประเด็นต่าง ๆ รวมถึงความสอดคล้องกับกฎระเบียบหรือข้อบังคับที่เกี่ยวข้อง นอกจากนี้ ควรเพิ่มการมีส่วนร่วมของมนุษย์ในกระบวนการทำงานร่วมกับ Generative AI และหมั่นอัปเดตการเปลี่ยนแปลงทางด้านเทคโนโลยีเพื่อให้มั่นใจว่าการประยุกต์ใช้มีความสอดคล้องกับความสามารถของเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง ทั้งนี้ เพื่อเป็นการเตรียมพร้อมรับมือกับข้อจำกัดต่าง ๆ ของ Generative AI ได้อย่างมีประสิทธิภาพ

6.3 ความเสี่ยงของ Generative AI

6.3.1 ความเสี่ยงที่อาจเกิดขึ้นจากการประยุกต์ใช้ Generative AI

การทำความเข้าใจประเด็นความเสี่ยงที่อาจเกิดขึ้นเมื่อนำเทคโนโลยี Generative AI มาประยุกต์ใช้ในองค์กรจะช่วยให้องค์กรหาสมดุลระหว่างประโยชน์และความเสี่ยง ทำให้สามารถตัดสินใจนำ Generative AI มาประยุกต์ใช้งานได้อย่างเหมาะสม

Generative AI นำมาซึ่งความเสี่ยงรูปแบบใหม่ ดังนั้น องค์กรจึงควรมีวิธีการวิเคราะห์และจัดการความเสี่ยงเพิ่มเติมอย่างเหมาะสม โดยจากเอกสาร "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile" ของ National Institute of Standards and Technology (NIST) ซึ่งมีการระบุประเด็นความเสี่ยงที่ควรให้ความสำคัญ ซึ่งประกอบด้วย

1) **ความเสี่ยงด้านเนื้อหาที่น่าเชื่อถือแต่ไม่ถูกต้อง (Confabulation):** การผลิตเนื้อหาที่ดูน่าเชื่อถือแต่ไม่ถูกต้องตามข้อเท็จจริง อาจถูกเรียกว่า **“Hallucination”** หรือ **“Fabrication”** โดย Generative AI อาจสร้างผลลัพธ์ที่ผิดไปจากข้อเท็จจริง หรือขัดแย้งกับข้อความที่สร้างขึ้นก่อนหน้าทั้งที่อยู่บนบริบทเดียวกัน เช่น สับสนเกี่ยวกับบุคคล สถานที่ หรือรายละเอียดเหตุการณ์ทางประวัติศาสตร์ เป็นต้น ซึ่งอาจทำให้เกิดการนำเนื้อหาที่ผิดไปใช้งาน
2) **ความเสี่ยงด้านเนื้อหาอันตรายหรือรุนแรง (Dangerous or Violent Recommendations):** Generative AI อาจให้คำแนะนำที่ยั่วยุ ปลุกปั่น หรือคุกคาม ที่จะนำไปสู่ความรุนแรง โดยอาจ สร้างภาพ วิดีโอ หรือเสียง เพื่อให้เกิดความเข้าใจผิดในตัวองค์กรหรือบุคคล และอาจนำไปสู่การกระทำผิดทางกฎหมาย
3) **ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูล (Data Privacy):** ข้อมูลที่ใช้ในการฝึกฝนโมเดล Generative AI อาจถูกเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ส่งผลกระทบต่อความเป็นส่วนตัวได้ เช่น ข้อมูลบัตรประชาชน ประวัติการรักษา ที่อยู่ หรือข้อมูลที่สามารถระบุตัวตนได้ เป็นต้น ซึ่งข้อมูลดังกล่าวอาจรั่วไหลจากการโจมตี หรือเป็นส่วนหนึ่งของผลลัพธ์ นอกจากนี้ ผลลัพธ์ที่ปรากฏข้อมูลส่วนบุคคลอาจทำให้เกิดผลลัพธ์ที่มีอคติและการเลือกปฏิบัติที่เป็นอันตรายต่อตัวบุคคลได้
4) **ความเสี่ยงด้านการทำงานร่วมกันระหว่างมนุษย์และ Generative AI (Human-AI Configuration):** การกำหนดระดับการมีส่วนร่วมหรือปฏิสัมพันธ์ระหว่างมนุษย์และระบบ AI อาจก่อให้เกิดความเสี่ยง เช่น การอคติหรือไม่เชื่อผลลัพธ์ การเชื่อผลลัพธ์มากเกินไปโดยไม่ตรวจสอบ ความไม่สอดคล้องกับเป้าหมายและ/ผลลัพธ์ที่ต้องการ การใช้ในทางที่ผิด การใช้อย่างไม่ถูกต้อง และใช้อย่างไม่ปลอดภัยกับมนุษย์ เป็นต้น
5) **ความเสี่ยงด้านการนำข้อมูลที่ไม่ครบถ้วนถูกต้อง หรือบิดเบือน (Information Integrity):** Generative AI อาจถูกใช้เป็นเครื่องมือในการสร้างและเผยแพร่ข้อมูลที่ไม่ถูกต้อง (misinformation) หรือข้อมูลที่ถูกทำให้บิดเบือน (disinformation) ซึ่งอาจทำลายความเชื่อมั่นต่อบุคคล องค์กร และสังคมในวงกว้าง
6) **ความเสี่ยงด้านความปลอดภัยของข้อมูล (Information Security):** ผู้ไม่หวังดีอาจใช้ Generative AI ในการหาช่องโหว่ของระบบ การเขียนโปรแกรมในการเจาะระบบขององค์กร นอกจากนี้ Generative AI เองยังเป็นเป้าหมายในการถูกโจมตี เช่น การโจมตีที่โมเดลโดยตรง โดยเฉพาะ

การเขียนโจมตีแบบ Prompt injection หรือ การแก้ไขข้อมูลที่ใช้ฝึกฝนโมเดล (Data Poisoning) ซึ่งส่งผลให้ Generative AI ทำงานผิดพลาด

7) **ความเสี่ยงด้านทรัพย์สินทางปัญญา (Intellectual Property):** ผลลัพธ์ที่มาจาก Generative AI อาจละเมิดทรัพย์สินทางปัญญา เนื่องจากการจำข้อมูลหรือการสร้างเนื้อหาที่คล้ายกับผลงานที่ได้รับความคุ้มครองลิขสิทธิ์ รวมถึงการใช้อัตลักษณ์หรือลักษณะเด่นของบุคคลที่ไม่ได้รับอนุญาตอาจเป็นปัญหาที่ไม่ได้รับการคุ้มครองจากกฎหมายทรัพย์สินทางปัญญา
8) **ความเสี่ยงด้านเนื้อหาลามก คุกคามหรือล่วงละเมิดทางเพศ (Obscene, Degrading, and/or Abusive Content):** Generative AI มีโอกาสสร้างเนื้อหาลามกอนาจาร คุกคามหรือล่วงละเมิดทางเพศ เนื่องจากโมเดล AI ถูกฝึกฝนด้วยชุดข้อมูลเปิดในอินเทอร์เน็ตที่อาจมีเนื้อหาลักษณะดังกล่าว รวมถึงข้อมูลที่ไม่ได้รับอนุญาต ดังนั้น ผลลัพธ์ที่ถูกสร้างขึ้นอาจส่งผลกระทบทางจิตใจและร่างกายของบุคคลที่เกี่ยวข้อง
9) **ความเสี่ยงด้านเนื้อหาที่มีความคิดเชิงลบ อคติ แบ่งแยก (Toxicity, Bias, and Homogenization):** Generative AI มีโอกาสสร้างเนื้อหาที่มีความคิดเชิงลบ อคติ หรือแบ่งแยก ที่อาจถูกเผยแพร่เป็นวงกว้างและไม่สามารถควบคุมการแพร่กระจายได้ง่ายซึ่งอาจก่อให้เกิดความเสียหายแก่ชื่อเสียงและจิตใจของบุคคลที่เกี่ยวข้องได้
10) **ความเสี่ยงโดยรวมของห่วงโซ่อุปทาน (Value Chain and Component Integration):** โมเดล Generative AI อาจถูกฝึกฝนด้วยเนื้อหาที่ไม่ได้รับการตรวจสอบจากแหล่งที่มาของบุคคลที่สาม ซึ่งอาจทำให้ผลลัพธ์ของโมเดลไม่สามารถตรวจสอบได้ และอาจจะก่อให้เกิดความเสี่ยงต่อผู้ที่เกี่ยวข้องในห่วงโซ่อุปทาน
11) **ความเสี่ยงด้านสิ่งแวดล้อม (Environmental):** ความเสี่ยงด้านสิ่งแวดล้อมจากการใช้ทรัพยากรจำนวนมากในการฝึกโมเดล อาจสร้างผลกระทบด้านพลังงานและการปล่อยคาร์บอนของ Generative AI ซึ่งขึ้นอยู่กับประเภทของโมเดล, รูปแบบ, ฮาร์ดแวร์ และประเภทของแอปพลิเคชัน
12) **ความเสี่ยงด้านข้อมูลที่เป็นอันตรายต่อการผลิตอาวุธเคมี รังสี หรือนิวเคลียร์ (Chemical, Biological, Radiological, or Nuclear (CBRN) Weapons):** Generative AI อาจถูกใช้เป็นเครื่องมือในการสร้างเนื้อหาที่เกี่ยวข้องกับการผลิตอาวุธเคมี รังสี หรือนิวเคลียร์ และอาจนำไปใช้ในทางที่ไม่เหมาะสม

การวิเคราะห์ประเด็นความเสี่ยงของการประยุกต์ใช้ Generative AI ควรพิจารณาโอกาสความเป็นไปได้ (Likelihood) และผลกระทบ (Impact) ที่อาจเกิดขึ้นในมิติต่าง ๆ ดังนั้น องค์กรควรหมั่นติดตามข้อมูลที่เกี่ยวข้องกับเทคโนโลยีและการพัฒนาของ Generative AI เพื่อนำมาทบทวนแนวทางจัดการความเสี่ยงที่อาจเกิดขึ้นจากการประยุกต์ใช้ Generative AI อย่างเหมาะสมต่อไป

6.3.2 แนวทางการบริหารจัดการความเสี่ยง

Generative AI มีความสามารถที่แตกต่างไปจาก AI ประเภทอื่นจึงนำมาซึ่งความเสี่ยงรูปแบบใหม่ ดังนั้นในการประยุกต์ใช้ Generative AI จึงควรคำนึกถึงประเด็นความเสี่ยงที่เกี่ยวข้องและกำหนดมาตรการเพื่อป้องกันหรือลดความเสี่ยงที่อาจจะเกิดขึ้นอย่างเหมาะสม โดยแนวทางในการจัดการความเสี่ยงในการประยุกต์ใช้ Generative AI นั้นมีหลากหลายแนวทาง โดยยกตัวอย่าง ดังนี้

1) **กำหนดกรอบแนวทางประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาล (Establish Generative AI Governance Structure):** องค์กรควรกำหนดกรอบแนวทางในการประยุกต์ใช้ Generative AI ที่ครอบคลุมรูปแบบและลักษณะการประยุกต์ใช้งานจริงภายในองค์กร ทั้งนี้ โดยควรพิจารณาประเด็นความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้น และกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) รวมถึงกำหนดความรับผิดชอบต่อผลของการกระทำ (Accountability) ในการประยุกต์ใช้ Generative AI
2) **หมั่นตรวจสอบและทบทวนความสอดคล้องตามข้อกำหนด หรือข้อกฎหมาย (Ensure Regulatory and Legal Compliance):** ที่เกี่ยวข้องกับการประยุกต์ใช้ Generative AI ว่ายังเป็นไปตามข้อกำหนดหรือข้อกฎหมายหรือไม่ โดยอาจจำเป็นต้องปรับปรุงกฎระเบียบภายในองค์กรให้ทันสมัยอยู่เสมอ ทั้งนี้ ในบางกรณีอาจต้องมีการปรับปรุงระบบให้สอดคล้องกับกฎ ระเบียบ หรือกฎหมายที่เกี่ยวข้อง
3) **ส่งเสริมการประยุกใช้ Generative AI อย่างมีจริยธรรม (Foster a Culture of Ethical Generative AI):** พัฒนาองค์ความรู้บุคลากรในการใช้งาน Generative AI อย่างรู้เท่าทัน สร้างความเข้าใจเกี่ยวกับประเด็นด้านจริยธรรมและแนวปฏิบัติที่ดีในการประยุกต์ใช้ Generative AI พร้อมทั้งมีมาตรการตรวจสอบว่ามีการปฏิบัติตามแนวทางที่ดีที่องค์กรกำหนดไว้
4) **กำหนดแนวทางการทำงานร่วมกันระหว่างมนุษย์และ Generative AI (Ensure Human Oversight):** สร้างแนวทางการทำงานร่วมกันระหว่างมนุษย์และ Generative AI เพื่อหลีกเลี่ยงการพึ่งพา Generative AI มากเกินไป โดยเพิ่มบทบาทการมีส่วนร่วมของมนุษย์ในกระบวนการทำงานกับ Generative AI ซึ่งจะช่วยลดความเสี่ยงจากความผิดพลาดของ Generative AI
5) **สร้างความร่วมมือระหว่างฝ่ายงานต่าง ๆ ในองค์กร (Promote Interdisciplinary Collaboration):** ส่งเสริมการบูรณาการ การทำงานระหว่างฝ่ายต่าง ๆ ในการพัฒนาและใช้งาน Generative AI ตั้งแต่ประเมินความเสี่ยงไปจนถึงการออกแบบกลยุทธ์บริหารจัดการความเสี่ยง
6) **พัฒนาแนวทางกำกับดูแลด้านข้อมูลองค์กร (Enhance Data Governance):** จัดทำกรอบแนวทางการกำกับดูแลการนำข้อมูลไปใช้กับ Generative AI อย่างเหมาะสม โดยคำนึงถึงความสอดคล้องกับหลักจริยธรรม AI การจัดการข้อมูลที่เป็นระบบ การตรวจสอบความถูกต้อง การปกป้องความเป็นส่วนตัว การทำความเข้าใจบริบทของข้อมูลก่อนนำไปฝึกฝนโมเดล การนำข้อมูลไปใช้งานกับ Generative AI ทั้งนี้ ควรตรวจสอบการกำกับดูแลข้อมูลในประเด็นต่าง ๆ ข้างต้นอย่างสม่ำเสมอ
7) **เฝ้าติดตาม ประเมินผล และปรับปรุงการใช้งาน (Monitor, Evaluate, and Improve):** ควรมีการประเมินผลทั้งก่อนและหลังการนำ Generative AI ไปใช้จริงในองค์กร เพื่อให้แน่ใจว่าการใช้งานเป็นไปตามเป้าหมายในบริบทสถานการณ์จริง และมีกลไกช่องทางการรับฟังความคิดเห็น (Feedback) จากผู้ใช้งานและนำมาปรับปรุงระบบให้มีประสิทธิภาพ
8) **ประเมินและตรวจสอบผลิตภัณฑ์หรือบริการที่เกี่ยวข้องจากหน่วยงานภายนอก (Monitor and Evaluate Products/Services by External Parties):** ประเมินความเสี่ยงและตรวจสอบผลิตภัณฑ์หรือบริการ (เช่น เครื่องมือ โมเดล และชุดข้อมูล) จากหน่วยงานภายนอก เพื่อให้แน่ใจว่ามีความสอดคล้องตามนโยบายการจัดการความเสี่ยงขององค์กร รวมถึงมีการติดตามประสิทธิภาพอย่างสม่ำเสมอ เพื่อให้สามารถรับรู้ถึงความเสี่ยงใหม่ที่อาจจะเกิดและปรับแผนจัดการความเสี่ยงตามความจำเป็นเหมาะสม

9) **กำหนดมาตรการและเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ (Establish Cyber Security Mechanisms):** จัดทำมาตรการการรักษาความปลอดภัยทางไซเบอร์ เพื่อป้องกันการเข้าถึงข้อมูลและระบบโดยไม่ได้รับอนุญาต (Unauthorized Access) การเจาะระบบ (Hacking) การละเมิดข้อมูล (Data Breaches) การรั่วไหลข้อมูล (Data Leakage) เข้ารหัสข้อมูลสำคัญ อัปเดตโปรโตคอลความปลอดภัยและตรวจสอบสิทธิ์การเข้าถึงเป็นประจำ

ทั้งนี้ สามารถกำหนดมาตรการบริหารจัดการความเสี่ยงอื่น ๆ เพิ่มเติมตามความเหมาะสมและสอดคล้องกับเป้าหมายที่กำหนดได้

ตัวอย่างการควบคุมและการจัดการความเสี่ยง: Chatbot ช่วยตอบคำถามแทนฝ่ายทรัพยากรบุคคล

รายละเอียดของ Scenario

องค์กรได้นำเอา Generative AI Chatbot มาช่วยงานฝ่ายทรัพยากรบุคคล (HR) ขององค์กรในการตอบคำถามของพนักงาน โดย Chatbot ได้รับการออกแบบมาเพื่อช่วยตอบคำถามหลาย ๆ ด้านเกี่ยวกับสิทธิสวัสดิการและผลประโยชน์ที่พนักงานจะได้รับ การจ่ายเงินเดือน ตลอดจนผลการปฏิบัติงาน เป็นต้น

แม้ว่า Chatbot ข้างต้นจะสามารถสนับสนุนพนักงานภายในองค์กร และช่วยลดภาระงานให้แก่เจ้าหน้าที่ฝ่ายทรัพยากรบุคคล แต่อย่างไรก็ตาม ได้มีพนักงานจำนวนหนึ่งแจ้งปัญหาของ Chatbot กรณีที่สร้างเนื้อหาคำตอบที่ไม่ถูกต้อง รวมถึงมีการเปิดเผยข้อมูลที่มีความลับ อาทิ รายงานการประเมินผลการปฏิบัติงาน หรือข้อมูลส่วนบุคคล

ตัวอย่างความเสี่ยงที่อาจเกิดขึ้น

- **ความเสี่ยงด้านเนื้อหาที่น่าเชื่อถือแต่ไม่ถูกต้อง (Confabulation)** Generative AI Chatbot ตอบข้อมูลพนักงาน โดยใช้ข้อมูลสวัสดิการของพนักงานที่ไม่มีอยู่จริงตามที่ระบุในเอกสาร
- **ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูล (Data Privacy)** Generative AI Chatbot ตอบคำถามพนักงานโดยนำข้อมูลส่วนบุคคลของพนักงานคนหนึ่ง มาตอบคำถามแก่พนักงานอีกคนหนึ่ง

ตัวอย่างแนวทางการจัดการความเสี่ยง

- **เฝ้าติดตาม ประเมินผล และปรับปรุงการใช้งาน (Monitor, Evaluate, and Improve)** สร้างกระบวนการหรือช่องทางเพื่อรับฟังความเห็นจากผู้ใช้งาน (Feedback Loop) เกี่ยวกับผลลัพธ์ของ Generative AI Chatbot เช่น เพิ่มปุ่มให้พนักงานสามารถเลือกเพื่อให้ความเห็นว่าคำตอบของ Generative AI Chatbot ถูกต้องเหมาะสมหรือไม่ และนำข้อมูลความเห็นนั้นมาประเมินสาเหตุและปรับปรุงผลลัพธ์ของ Generative AI Chatbot เช่น Retrieval-Augmented Generation (RAG) เป็นต้น
- **พัฒนาแนวทางกำกับดูแลด้านข้อมูลองค์กร (Enhance Data Governance)** องค์กรควรกำหนดนโยบายมาตรการควบคุมการเข้าถึงข้อมูลและความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลอ่อนไหวโดยไม่ได้รับอนุญาต รวมไปถึงกำหนดรูปแบบของข้อมูลที่เหมาะสมในการนำมาใช้งานร่วมกับ Generative AI อย่างชัดเจน

6.4 แนวปฏิบัติสำหรับการประยุกต์ใช้ Generative AI

6.4.1 การประยุกต์ใช้ Generative AI สำหรับการดำเนินงานตามภารกิจขององค์กร

1) การประยุกใช้ Generative AI ต้องเป็นไปเพื่อประโยชน์ขององค์กร และสอดคล้องตามภารกิจขององค์กรเท่านั้น
2) ผู้ใช้งานต้อง ***<u>ไม่ใช่</u>*** Generative AI ในการ
   - สร้างเนื้อหาที่ผิดกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง
   - สร้างเนื้อหาที่เป็นอันตราย ทำให้เสื่อมเสียชื่อเสียง หรือเนื้อหาที่เป็นการล่วงละเมิดหรือไม่เหมาะสม
   - สร้างและแจกจ่ายเนื้อหาที่มีเจตนาบิดเบือน แสดงข้อมูลไม่ถูกต้องหรือทำให้ผู้อื่นเข้าใจผิด
   - ดำเนินการใด ๆ ให้กิจกรรมหรือบริการขององค์กร หยุดชะงัก ระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

6.4.2 การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล

ด้วยแอปพลิเคชันหรือบริการ Generative AI ที่ให้บริการ โดยเฉพาะอย่างยิ่งแอปพลิเคชันหรือบริการที่ไม่มีค่าใช้จ่าย ผู้ใช้งานต้องมีความระมัดระวังและปฏิบัติตามแนวปฏิบัติ ดังต่อไปนี้

1) ไม่นำข้อมูลภายในองค์กรและข้อมูลที่มีชั้นความลับ (เช่น รหัสผ่าน เอกสารสัญญา เอกสารหรือหนังสือที่ประทับข้อความลับ เอกสารหรือข้อมูลเกี่ยวกับโครงการภายในองค์กร ฯลฯ) ไปใช้งานร่วมกับแอปพลิเคชันหรือบริการ Generative AI
2) ไม่นำข้อมูลส่วนบุคคล (เช่น รูปภาพบุคคล ชื่อ-สกุล หมายเลขประจำตัวประชาชน ที่อยู่ หมายเลขโทรศัพท์ อีเมล ฯลฯ) และข้อมูลส่วนบุคคลที่อ่อนไหว (เช่น สำเนาบัตรประชาชนที่มีข้อมูลศาสนา ข้อมูลชีวภาพ ใบรับรองแพทย์ ฯลฯ) ไปใช้งานร่วมกับแอปพลิเคชันหรือบริการ Generative AI
3) ในกรณีที่ต้องใช้แอปพลิเคชันหรือบริการ Generative AI ร่วมกับข้อมูลภายในองค์กร ข้อมูลที่มีชั้นความลับ ข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลที่อ่อนไหว จะต้องใช้แอปพลิเคชันหรือบริการที่ได้รับการอนุมัติโดยผู้บังคับบัญชาหรือจัดหาโดยองค์กร เท่านั้น

6.4.3 การรักษาความมั่นคงปลอดภัย

1) ไม่นำข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบ (เช่น รหัสผ่าน ข้อมูล API Key รายละเอียดการตั้งค่าของระบบ ฯลฯ) ไปใช้งานร่วมกับแอปพลิเคชันหรือบริการ Generative AI
2) ต้องตรวจสอบซอร์สโค้ดที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำมาใช้งาน โดยพิจารณาถึงความถูกต้อง และการตรวจสอบช่องโหว่อย่างถี่ถ้วน
3) หากพบเหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดจากการประยุกต์ใช้ Generative AI ผู้ใช้งานต้องแจ้งให้ผู้บังคับบัญชารับทราบ และปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ หมวดที่ 8 การป้องกันและรับมือเหตุละเมิดด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ โดยทันที

6.4.4 การลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มบุคคล

ด้วยผลลัพธ์จากแอปพลิเคชันหรือบริการ Generative AI ที่ให้บริการ อาจก่อให้เกิดอคติและการเลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล ดังนั้น ผู้ใช้งานจึงต้องมีความระมัดระวังและปฏิบัติตามแนวปฏิบัติ ดังต่อไปนี้

1) ต้องตรวจสอบเนื้อหาที่สร้างโดย Generative AI ก่อนนำไปใช้งานหรือเผยแพร่ต่อสาธารณะ เพื่อลดหรือหลีกเลี่ยงการเกิดอคติหรือการเลือกปฏิบัติอย่างไม่เป็นธรรม
2) ในกรณีที่ใช้แอปพลิเคชันหรือบริการ Generative AI สำหรับการดำเนินงานที่อาจกระทบต่อสิทธิของบุคคลหรือกลุ่มบุคคลโดยตรง ผู้ใช้งานจะต้องใช้ความระมัดระวังเท่าที่จะต้องใช้และสมควรจะต้องใช้สำหรับการดำเนินการดังกล่าว

6.4.5 เคารพสิทธิในทรัพย์สินทางปัญญา

1) ในการนำเนื้อหาที่สร้างโดย Generative AI ไปใช้งานหรือเผยแพร่ต่อสาธารณะ ผู้ใช้งานต้องใช้แอปพลิเคชันหรือบริการที่ได้รับการอนุมัติโดยผู้บังคับบัญชาหรือจัดหาโดยองค์กร เท่านั้น
2) การประยุกต์ใช้ Generative AI ด้วยความประมาทอาจทำให้เกิดการละเมิดสิทธิในทรัพย์สินทางปัญญาได้ ดังนั้น ผู้ใช้งาน Generative AI จึงต้องมีความระมัดระวังไม่ให้เกิดการละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือสิทธิในทรัพย์สินทางปัญญาอื่น ๆ

6.5 ข้อห้ามในการใช้เทคโนโลยี Generative AI

1) ห้ามใช้ในทางที่ขัดต่อหลักธรรมาภิบาล คุณธรรม จริยธรรม ศีลธรรม หรือมีเจตนาแอบแฝงโดยไม่สุจริต
2) ห้ามใช้แทนการตัดสินใจของผู้ใช้งานในกรณีที่มีความเสี่ยงสูง เช่น การตัดสินใจทางกฎหมาย ทางการแพทย์ ทางการเงิน หรือการตัดสินใจที่อาจส่งผลกระทบต่อชีวิต ทรัพย์สินและสิทธิของบุคคล
3) ห้ามใช้เพื่อสร้างข้อมูลอันเป็นเท็จ หรือสร้างเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล องค์กร หรือสังคม อันอาจนำไปสู่ความเข้าใจผิด หรือสร้างความขัดแย้งในสังคม
4) ห้ามใช้หรือเปิดเผยข้อมูลที่เป็นความลับขององค์กร รวมถึงข้อมูลภายในเอกสารสำคัญ หรือข้อมูลที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กร
5) ห้ามใช้ข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือใช้ข้อมูลที่อาจเป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง
6) ห้ามใช้เพื่อสร้างเนื้อหาที่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา รวมถึงการทำซ้ำ คัดลอก หรือ ดัดแปลงซึ่งเนื้อหาที่เป็นของบุคคลหรือหน่วยงานอื่นโดยไม่ได้รับอนุญาต
7) ห้ามใช้เพื่อสร้างเนื้อหาที่ส่งเสริมการเหยียดเชื้อชาติ ศาสนา เพศ วัย ความพิการ หรือสถานะทางสังคม ซึ่งอาจขัดต่อกฎหมายและหลักสิทธิมนุษยชน
8) ห้ามใช้ในการดำเนินการใด ๆ ที่อาจเป็นการกระทำความผิดตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง หลักเกณฑ์ หรืออื่น ๆ ที่เกี่ยวข้อง

6.6 หน้าที่และความรับผิดชอบในการประยุกต์ใช้ Generative AI

การใช้งานเนื้อหาที่สร้างโดย Generative AI อาจส่งผลกระทบเชิงลบต่อบุคคล องค์กร และสังคม โดย**องค์กรและผู้ใช้งานไม่อาจปฏิเสธความรับผิดต่อผลของการกระทำ (Accountability)** ดังกล่าวได้ ด้วยเหตุนี้ ผู้ใช้งานและบุคคลที่เกี่ยวข้องกับการประยุกต์ใช้ Generative AI จึงมีหน้าที่และความรับผิดชอบในการประยุกต์ใช้ Generative AI ดังต่อไปนี้

1) ผู้ใช้งานต้องใช้เทคโนโลยี Generative AI อย่างมีธรรมาภิบาล มีจริยธรรม มีความมั่นคงปลอดภัย สอดคล้องตามกฎหมาย และข้อกำหนดที่เกี่ยวข้อง
2) ผู้ใช้งานต้องทำการศึกษาข้อมูลเทคโนโลยี Generative AI เพื่อสร้างความเข้าใจเกี่ยวกับข้อมูลพื้นฐาน ศักยภาพ ประโยชน์ ความเสี่ยง และข้อจำกัด เพื่อให้ผู้ใช้งานสามารถประยุกต์ใช้เทคโนโลยี Generative AI ได้อย่างเหมาะสม มีประสิทธิภาพและสอดคล้องกับเป้าหมายของงานแต่ละประเภทที่ได้รับมอบหมาย
3) ผู้ใช้งานต้องแจ้งผู้บังคับบัญชาอย่างชัดเจนเกี่ยวกับวัตถุประสงค์ ขอบเขต และการทำงานร่วมกันระหว่างผู้ใช้งานกับ Generative AI (AI Human Involvement) เมื่อใช้ Generative AI ในการปฏิบัติงาน รวมทั้งแจ้งพนักงานหรือลูกจ้างให้ทราบว่าข้อมูลใดเกิดจากการประยุกต์ Generative AI
4) ผู้ใช้งานต้องตรวจสอบเนื้อหาที่สร้างโดย Generative AI ก่อนนำไปใช้งานหรือเผยแพร่ โดยในการตรวจสอบผู้ใช้งานจำเป็นต้องพิจารณาในประเด็น ดังต่อไปนี้
   - ความถูกต้องของเนื้อหา
   - ผลของการใช้งานหรือเผยแพร่เนื้อหาที่นำไปสู่การกระทำผิดทางกฎหมาย รวมถึงการละเมิดทรัพย์สินทางปัญญา
   - ความเท่าเทียมและการไม่เลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล
   - การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล
   - ผลกระทบต่อความมั่นคงปลอดภัย
   - ผลกระทบเชิงลบอื่น ๆ ที่อาจเกิดขึ้นต่อบุคคล องค์กร และสังคม
5) ผู้ใช้งานต้องรายงานให้ผู้บังคับบัญชารับทราบโดยทันที ในกรณีที่การประยุกต์ใช้ Generative AI เกิดความผิดพลาดหรือพบประเด็นปัญหาทั้งกรณีการนำเข้าข้อมูลและแสดงผลลัพธ์ที่อาจส่งผลกระทบเชิงลบต่อบุคคล องค์กร และสังคม
6) ผู้บังคับบัญชาและผู้ใช้งานต้องมีการทบทวนประเด็นปัญหา ประเมินประสิทธิภาพและประสิทธิผลของการประยุกต์ใช้ Generative AI เพื่อปรับปรุงวิธีการทำงานและเลือกใช้แอปพลิเคชันหรือบริการที่เหมาะสมกับการปฏิบัติงาน
7) การพิจารณาและอนุมัติรายการแอปพลิเคชันหรือบริการ Generative AI ที่เหมาะสมสำหรับการใช้งานภายในองค์กร ให้ถือปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ หมวดที่ 6 การควบคุมการเข้าถึง ข้อ 6.8 การควบคุมการใช้งานระบบสารสนเทศ (Information System) โปรแกรมประยุกต์ (Application Software) และโปรแกรมอรรถประโยชน์ (Utility Program)

7 กฎหมาย กฎระเบียบ นโยบาย และแนวปฏิบัติที่เกี่ยวข้อง

1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

กฎหมายฉบับนี้เป็นกฎหมายหลักในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศ หากนำระบบปัญญาประดิษฐ์ไปใช้ในหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure – **CII**) ระบบดังกล่าวจะต้องผ่านมาตรฐานและมาตรการด้านความปลอดภัยตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กำหนด

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act: PDPA)

กฎหมายฉบับนี้มีความสำคัญอย่างยิ่งต่อการพัฒนาและใช้งานปัญญาประดิษฐ์ เนื่องจากระบบปัญญาประดิษฐ์ โดยเฉพาะ Machine Learning ต้องใช้ข้อมูลจำนวนมากในการฝึกสอน ประเด็นที่ต้องพิจารณาอย่างเคร่งครัด ได้แก่

2.1) ฐานทางกฎหมายในการประมวลผล การรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อฝึกสอนปัญญาประดิษฐ์ ต้องมีฐานทางกฎหมายรองรับ ซึ่งส่วนใหญ่มักจะเป็น “ความยินยอม” จากเจ้าของข้อมูล

2.2) สิทธิ์ของเจ้าของข้อมูล องค์กรต้องมีช่องทางให้เจ้าของข้อมูลสามารถใช้สิทธิ์ของตนได้ เช่น สิทธิ์ในการเพิกถอนความยินยอม หรือสิทธิ์ในการคัดค้านการประมวลผล

2.3) มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล องค์กรมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่นำมาใช้กับปัญญาประดิษฐ์อย่างเหมาะสม เพื่อป้องกันการรั่วไหลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

3) แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

4) นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ กทท.

5) นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ กทท.

6) นโยบายการกำกับดูแลข้อมูลของ กทท.

7) นโยบายการบริหารความเสี่ยงและควบคุมภายในของ กทท.

8) นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ กทท.

เอกสารอ้างอิง

1) หลักการแนวทางจริยธรรมปัญญาประดิษฐ์ (Thailand AI Ethics Guideline) ของ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ตามมติคณะรัฐมนตรี เมื่อวันที่ 2 กุมภาพันธ์ 2564
2) แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาลสำหรับผู้บริหารองค์กร ของ สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เผยแพร่เมื่อวันที่ 12 ธันวาคม 2566
3) แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร ของ สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เผยแพร่เมื่อวันที่ 30 ตุลาคม 2567
4) แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย ของ สำนักคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เผยแพร่เมื่อวันที่ 1 ตุลาคม 2568