



WHA GROUP

Standard

มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ (AI Management Standard)

Document Properties

Document Number	WHACG-ICT-STND-0008
Softcopy Location	CDMS / WHA SharePoint
Owner Division	IT Department
Owner Department	IT Department
Version Number	v1.1.0 (Approved Final)
Release Date	28 Aug 2026

Document Approval

Approver

Jareeporn Jarukornsakul
(Chairman of the Executive Committee and
Group Chief Executive Officer)

Pajongwit Pongsivapai
(Chief Executive Officer – WHA Industrial Development)

Akarin Prathuangsit
(Chief Executive Officer – WHA Utilities and Power)

Nunsilp Janvarin
(Acting Chief Executive Officer – WHA Digital)

Reviewer

Nunsilp Janvarin
(Chief Technology Officer)

Nattapong Kanyanutcharat
(Director - IT Department)

Patcharin Tongaree
(Data and AI Deputy Director - IT Department)

Owner

Soros Sottitavorn
(Infrastructure and Cybersecurity Deputy Director - IT Department)

Document Control

การเปลี่ยนแปลงเอกสาร:

รายการบันทึกการเปลี่ยนแปลงเอกสาร

เวอร์ชัน	วันที่อนุมัติ	เจ้าของเอกสาร	การเปลี่ยนแปลง
1.1.0	28 ส.ค. 2569	Soros Sottitavorn - Infrastructure and Cybersecurity Deputy Director	แก้ไขรายละเอียดข้อ 3.4.1 เกี่ยวกับ การลดผลกระทบต่อ สิ่งแวดล้อมให้อยู่ในระดับต่ำ (Low Ecological Footprint)
1.0.0	11 ส.ค. 2569	Soros Sottitavorn - Infrastructure and Cybersecurity Deputy Director	เวอร์ชันแรก

ผู้แต่ง:

รายชื่อผู้แต่งที่จัดทำเอกสารฉบับนี้ มีดังนี้

ชื่อ - นามสกุล	ตำแหน่ง
Soros Sottitavorn	Infrastructure and Cybersecurity Deputy Director

ผู้ตรวจทาน:

รายชื่อผู้ตรวจทานเอกสารฉบับนี้ มีดังนี้

ชื่อ - นามสกุล	ตำแหน่ง
Nunsilp Janvarin	Chief Technology Officer
Nattapong Kanyanutcharat	Director - IT Department
Patcharin Tongaree	Data and AI Deputy Director - IT Department

ผู้อนุมัติ:

รายชื่อผู้อนุมัติเอกสารฉบับนี้ มีดังนี้

ชื่อ - นามสกุล	ตำแหน่ง
Jareeporn Jarukornsakul	Chairman of the Executive Committee and Group Chief Executive Officer
Pajongwit Pongsivapai	Chief Executive Officer – WHA Industrial Development
Akarin Prathuangsit	Chief Executive Officer – WHA Utilities and Power
Nunsilp Janvarin	Acting Chief Executive Officer – WHA Digital

สารบัญ (Table of Contents)

1)	บทนำ (INTRODUCTION)	6
2)	วัตถุประสงค์ของการบริหารจัดการปัญญาประดิษฐ์ (AI MANAGEMENT OBJECTIVES)	7
3)	มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ (AI MANAGEMENT STANDARD)	8
3.1)	นโยบายที่เกี่ยวข้องกับ AI (Policies related to AI)	8
3.1.1)	นโยบาย AI (AI policy)	8
3.1.2)	ความสอดคล้องกับนโยบายขององค์กรอื่น ๆ (Alignment with other organizational policies)	8
3.1.3)	การทบทวนนโยบาย AI (Review of the AI policy)	9
3.2)	การจัดการภายในองค์กร (Internal organization)	9
3.2.1)	บทบาทและหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับ AI (AI roles and responsibilities)	9
3.2.2)	การรายงานข้อห่วงใยต่อบทบาทขององค์กรที่เกี่ยวข้องกับระบบ AI (Reporting of concerns)	15
3.3)	ทรัพยากรสำหรับระบบ AI (Resources for AI systems)	15
3.3.1)	การจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากร (Resource documentation)	16
3.3.2)	ทรัพยากรด้านข้อมูล (Data resources)	16
3.3.3)	ทรัพยากรด้านเครื่องมือ (Tooling resources)	16
3.3.4)	ทรัพยากรด้านระบบและอุปกรณ์คอมพิวเตอร์ (System and computing resources)	17
3.3.5)	ทรัพยากรด้านบุคคล (Human resources)	17
3.4)	การประเมินผลกระทบของระบบ AI (Assessing impacts of AI systems)	18
3.4.1)	กระบวนการประเมินผลกระทบของระบบ AI (AI system impact assessment process)	18
3.4.2)	การจัดทำเอกสารการประเมินผลกระทบของระบบ AI (Documentation of AI system impact assessments)	19
3.4.3)	การประเมินผลกระทบของระบบ AI ต่อบุคคลหรือกลุ่มของบุคคล (Assessing AI system impact on individuals or groups of individuals)	19
3.4.4)	การประเมินผลกระทบของระบบ AI ต่อสังคม (Assessing societal impacts of AI systems)	20
3.5)	วงจรชีวิตของระบบ AI (AI system life cycle)	21
3.5.1)	แนวทางการบริหารจัดการสำหรับการพัฒนาระบบ AI (Management guidance for AI system development)	21
3.5.1.1)	วัตถุประสงค์สำหรับการพัฒนาระบบ AI อย่างมีความรับผิดชอบ (Objectives for responsible development of AI system)	21
3.5.1.2)	กระบวนการสำหรับการออกแบบและพัฒนาระบบ AI อย่างมีความรับผิดชอบ (Processes for responsible AI system design and development)	22

3.5.2)	วงจรชีวิตของระบบ AI (AI system life cycle)	22
3.5.2.1)	การกำหนดความต้องการด้านระบบ (AI system requirements and specification)	22
3.5.2.2)	การจัดทำเอกสารการออกแบบและพัฒนาระบบ AI (Documentation of AI system design and development)	23
3.5.2.3)	การประเมินและตรวจสอบความถูกต้องของระบบ AI (AI system verification and validation)	23
3.5.2.4)	การนำระบบ AI ไปสู่การใช้งาน (AI system deployment)	24
3.5.2.5)	การใช้งานและการเฝ้าระวังการทำงานของระบบ AI (AI system operation and monitoring)	24
3.5.2.6)	การจัดทำเอกสารทางเทคนิคของระบบ AI (AI system technical documentation)	25
3.5.2.7)	การบันทึกข้อมูลล็อกของเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบ AI (AI system recording of event logs)	26
3.6)	ข้อมูลสำหรับระบบ AI (Data for AI systems)	27
3.6.1)	ข้อมูลสำหรับการพัฒนาและปรับปรุงระบบ AI (Data for development and enhancement of AI system)	27
3.6.2)	การจัดหาข้อมูลสำหรับระบบ AI (Acquisition of data)	27
3.6.3)	คุณภาพของข้อมูลสำหรับระบบ AI (Quality of data for AI systems)	28
3.6.4)	แหล่งที่มาของข้อมูล (Data provenance)	28
3.6.5)	การจัดเตรียมข้อมูล (Data preparation)	28
3.7)	ข้อมูลสำหรับผู้มีส่วนได้ส่วนเสียกับระบบ AI (Information for interested parties of AI systems)	29
3.7.1)	การจัดทำเอกสารของระบบและข้อมูลสำหรับผู้ใช้งาน (System documentation and information for users)	29
3.7.2)	การรายงานจากภายนอก (External reporting)	30
3.7.3)	การสื่อสารเหตุการณ์ผิดปกติ (Communication of incidents)	30
3.7.4)	ข้อมูลสำหรับผู้มีส่วนได้ส่วนเสีย (Information for interested parties)	30
3.8)	การใช้งานระบบ AI (Use of AI systems)	31
3.8.1)	กระบวนการสำหรับการใช้งานระบบ AI อย่างมีความรับผิดชอบ (Processes for responsible use of AI systems)	31
3.8.2)	วัตถุประสงค์ของการใช้งานระบบ AI อย่างมีความรับผิดชอบ (Objectives for responsible use of AI system)	31
3.8.3)	การใช้งานระบบ AI ตามที่องค์กรต้องการ (Intended use of the AI system)	32
3.9)	ความสัมพันธ์กับผู้ให้บริการภายนอกและลูกค้า (Third-party and customer relationships)	32
3.9.1)	การกำหนดความรับผิดชอบ (Allocating responsibilities)	33
3.9.2)	ผู้ให้บริการภายนอก (Suppliers)	33
3.9.3)	ลูกค้า (Customers)	33
4)	แนวทางการใช้เทคโนโลยี AI (ARTIFICIAL INTELLIGENCE)	35
4.1)	การใช้เทคโนโลยี AI สำหรับการดำเนินงานตามภารกิจขององค์กร	35
4.2)	ข้อห้ามในการใช้เทคโนโลยี AI	35

4.3)	การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล.....	36
4.4)	การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีนำเทคโนโลยี AI มาใช้งาน	37
4.5)	การลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มบุคคล.....	37
4.6)	หน้าที่และความรับผิดชอบ.....	37
4.7)	การเคารพสิทธิในทรัพย์สินทางปัญญา	38
4.8)	การจัดฝึกอบรมให้ความรู้เกี่ยวกับการประยุกต์ใช้เทคโนโลยี AI	38
4.9)	โทษของการไม่ปฏิบัติตาม.....	39
4.10)	ตัวอย่างพฤติกรรมที่ควรทำและไม่ควรทำ (Do's & Don'ts) ของการใช้งานเทคโนโลยี AI.....	39
5)	การอ้างอิงเชิงบรรทัดฐาน (NORMATIVE REFERENCES)	40
6)	คำศัพท์และคำจำกัดความ (TERMS AND DEFINITIONS)	41

1) บทนำ (Introduction)

ในยุคที่เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจและการสร้างนวัตกรรม องค์กรจำเป็นต้องมีแนวทางที่ชัดเจนในการบริหารจัดการปัญญาประดิษฐ์ (AI Management) เพื่อให้การใช้งานปัญญาประดิษฐ์เป็นไปอย่างมีประสิทธิภาพ โปร่งใส มีจริยธรรม และปลอดภัย มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ (AI Management Standard) จึงถูกกำหนดขึ้นเพื่อเป็นกรอบการดำเนินงานที่สอดคล้องกับกลยุทธ์ขององค์กรและมาตรฐานสากล เช่น ISO/IEC 42001

การใช้ AI แม้จะช่วยในการพัฒนาธุรกิจและสร้างมูลค่าเพิ่มให้กับองค์กร แต่ก็มีความเสี่ยงที่ต้องบริหารจัดการอย่างรอบคอบ ไม่ว่าจะเป็นความเสี่ยงด้านความถูกต้องของข้อมูล ความเป็นส่วนตัว ความปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล ดังนั้น มาตรฐานนี้จึงมุ่งเน้นการใช้ AI อย่างมีความรับผิดชอบและมีจริยธรรม โดยกำหนดหลักการสำคัญ ได้แก่ ความโปร่งใส ความยุติธรรม ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง มาตรฐานนี้ครอบคลุมถึงการดำเนินงานตามกระบวนการที่มั่นคงปลอดภัยและตรวจสอบได้ รวมถึงการประเมินและปรับปรุงอย่างต่อเนื่อง เพื่อให้มั่นใจว่าการใช้ AI จะช่วยเสริมสร้างความสามารถในการแข่งขัน สนับสนุนการเติบโตขององค์กรอย่างยั่งยืน และสร้างความเชื่อมั่นให้กับผู้ที่มีส่วนได้ส่วนเสีย

อย่างไรก็ตาม หากการนำเทคโนโลยี AI มาใช้โดยขาดความรับผิดชอบหรือขาดการกำกับดูแลอย่างเหมาะสม อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคล องค์กร สังคม และประเทศชาติ อาทิ เช่น

1) ความเสียหายที่เกิดจากข้อมูล อันเนื่องมาจาก

- (ก) ข้อมูลเท็จที่ไม่ได้ตั้งใจให้เกิดความเข้าใจผิด (Misinformation) และข้อมูลเท็จที่จงใจให้เกิด ความเข้าใจผิด (Disinformation)
- (ข) เนื้อหาของข้อมูลไม่ถูกต้องตามข้อเท็จจริง (Confabulation)
- (ค) เนื้อหาของข้อมูลมีความอันตรายหรือรุนแรง (Dangerous or Violent Recommendations)
- (ง) เนื้อหาของข้อมูลส่งผลกระทบต่อความเป็นส่วนตัวของข้อมูล (Data Privacy)
- (จ) เนื้อหาของข้อมูลส่งผลกระทบต่อประเด็นที่มีความอ่อนไหวและมีเนื้อหาที่ขัดต่อหลักจริยธรรม (Sensitive and Ethics Context)
- (ฉ) เนื้อหาที่มีข้อมูลที่ไม่ถูกต้องครบถ้วนหรือถูกทำให้บิดเบือน (Information Integrity)
- (ช) เนื้อหาของข้อมูลที่อาจก่อให้เกิดอคติ แบ่งแยกและการเลือกปฏิบัติ (Bias and Discrimination)
- (ซ) ข้อมูลส่วนบุคคลรั่วไหล (Personal Data Leakage)

2) การละเมิดทรัพย์สินทางปัญญา (Intellectual Property Infringement)

3) ความมั่นคงปลอดภัยของข้อมูล (Information Security)

4) ผลกระทบอื่น ๆ ที่อาจเกิดขึ้นจากเทคโนโลยี AI หรือเทคโนโลยีอื่นที่มีลักษณะเดียวกัน เป็นต้น

ดังนั้น มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ (AI Management Standard) ฉบับนี้จึงได้ถูกจัดทำขึ้นเพื่อให้การนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ในการดำเนินกิจกรรมของ WHA Group เป็นไปอย่างมีประสิทธิภาพ โปร่งใส สอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลปัญญาประดิษฐ์ของกลุ่มบริษัท หลักธรรมาภิบาล และเป็นไปตามกฎหมาย

2) วัตถุประสงค์ของการบริหารจัดการปัญญาประดิษฐ์ (AI Management Objectives)

มาตรฐานนี้จัดทำขึ้นโดยมีเนื้อหาสาระสำคัญที่สามารถนำไปเป็นแนวทางการจัดฝึกอบรม การให้ความรู้ การทราบถึงโทษของการไม่ปฏิบัติตามมาตรฐาน และตัวอย่างพฤติกรรมที่ควรทำและไม่ควรทำของการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) รวมถึงแอปพลิเคชันหรือบริการปัญญาประดิษฐ์ (AI) ที่องค์กรแนะนำ เพื่อให้บุคลากร พนักงาน ลูกจ้าง ผู้ปฏิบัติงานและผู้รับจ้างขององค์กรสามารถนำเทคโนโลยีปัญญาประดิษฐ์ (AI) ไปใช้งานได้อย่างถูกต้องเหมาะสมมีความรับผิดชอบและสามารถนำเทคโนโลยีดังกล่าวไปสร้างสรรค์งานได้อย่างปลอดภัย มีประสิทธิภาพ ตลอดจนป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานที่ไม่เหมาะสม ในการนี้องค์กรจึงได้กำหนดวัตถุประสงค์ไว้ ดังนี้

1. เพื่อให้บุคลากร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน และผู้รับจ้างขององค์กร มีแนวทางปฏิบัติในการใช้เทคโนโลยี AI อย่างถูกต้อง เหมาะสมและมีประสิทธิภาพ
2. เพื่อให้การใช้งานและการพัฒนา AI อย่างมีความรับผิดชอบ มีความมั่นคงปลอดภัยและมีจริยธรรม เป็นไปตามนโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลปัญญาประดิษฐ์ของกลุ่มบริษัท กฎหมาย กฎ ระเบียบ ประกาศ ข้อบังคับอื่น ๆ ที่เกี่ยวข้อง พร้อมทั้งป้องกันความเสี่ยงที่เกิดจากการใช้งาน AI ผิดวัตถุประสงค์หรือสร้างอคติ ที่ก่อให้เกิดผลกระทบกับบุคคล องค์กร สังคม และประเทศชาติ
3. เพื่อเสริมสร้างความตระหนักรู้และความเข้าใจเกี่ยวกับการใช้เทคโนโลยี AI อย่างมีความรับผิดชอบ รอบคอบ สามารถใช้งานได้อย่างถูกต้องเหมาะสมและเป็นไปตามแนวทางที่องค์กรกำหนดไว้

3) มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ (AI Management Standard)

เนื้อหามาตรฐาน และการดำเนินการ

3.1) นโยบายที่เกี่ยวข้องกับ AI (Policies related to AI)

วัตถุประสงค์ เพื่อกำหนดทิศทางและการให้การสนับสนุนการบริหารจัดการปัญญาประดิษฐ์ขององค์กร อย่างมีความรับผิดชอบ โปร่งใส และสอดคล้องตามความต้องการทางธุรกิจ

องค์กรได้จัดทำนโยบาย Cybersecurity, Information Security & Privacy and AI Governance Policy เพื่อกำหนดทิศทางและการบริหารจัดการปัญญาประดิษฐ์ขององค์กร และจัดทำ AI Management Standard ฉบับนี้ให้สอดคล้องตามข้อกำหนดมาตรฐานสากล

3.1.1) มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ (AI Management Standard)

มาตรฐานฉบับนี้จัดทำเพื่อใช้สำหรับการพัฒนาหรือการใช้งานระบบ AI อย่างมีความรับผิดชอบ

แนวทางการนำไปปฏิบัติ

มาตรฐานฉบับนี้ประกอบด้วย

- กลยุทธ์ทางธุรกิจ
- ค่านิยมและวัฒนธรรมขององค์กร
- ระดับความเสี่ยงที่องค์กรยอมรับได้
- ระดับความเสี่ยงของระบบ AI
- ข้อกำหนดของกฎหมายที่องค์กรต้องปฏิบัติตาม รวมทั้งสัญญาจ้างที่เกี่ยวข้อง
- สภาพแวดล้อมขององค์กร
- ผลกระทบของระบบ AI ต่อผู้มีส่วนได้ส่วนเสีย

มาตรฐานฉบับนี้ครอบคลุมเนื้อหา ดังนี้

- หลักการของ AI ซึ่งให้แนวทางในการดำเนินกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับ AI
- กระบวนการสำหรับการจัดการความเสี่ยงและข้อกเว้นที่มีต่อนโยบาย และมาตรฐาน AI

มาตรฐานฉบับนี้ได้มีการพิจารณากำหนดหัวข้อที่เฉพาะเจาะจงสำหรับองค์กรตามความจำเป็นหรือได้มีการอ้างอิงไปยังนโยบายอื่น ๆ ที่เกี่ยวข้องกับหัวข้อเหล่านี้

- ทรัพยากรและทรัพย์สินของ AI
- การประเมินผลกระทบของระบบ AI
- การพัฒนาระบบ AI

นอกจากนี้ มาตรฐานฉบับนี้ยังครอบคลุมไปถึงการพัฒนาระบบ การจัดซื้อจัดจ้าง และการใช้ระบบ AI

3.1.2) ความสอดคล้องกับนโยบายขององค์กรอื่น ๆ (Alignment with other organizational policies)

องค์กรต้องกำหนดนโยบายอื่น ๆ ที่เกี่ยวข้องกับนโยบาย และ/หรือ มาตรฐานด้านปัญญาประดิษฐ์ โดยต้องมีการประยุกต์ใช้เพื่อให้เป็นไปตามวัตถุประสงค์ที่เกี่ยวข้องกับระบบ AI ขององค์กร

แนวทางการนำไปปฏิบัติ

ขอบเขตงานของ AI มีการซ้อนทับกับขอบเขตงานอื่น ๆ เป็นจำนวนมาก เช่น ด้านคุณภาพ ด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ด้านความปลอดภัยต่อชีวิตและทรัพย์สิน ด้านความเป็นส่วนตัว ดังนั้นองค์กรควรที่จะทำการวิเคราะห์โดยละเอียดเพื่อดูว่านโยบายใดที่มีการซ้อนทับกัน และดำเนินการปรับปรุงนโยบายที่เกี่ยวข้องเหล่านั้น หรือรวมเนื้อหาหรือข้อกำหนดของ AI เข้าไปไว้เป็นส่วนหนึ่งของนโยบายเหล่านั้น

3.1.3) การทบทวนนโยบายและมาตรฐาน AI (Review of the AI policy/standard)

นโยบาย และ/หรือ มาตรฐานด้านปัญญาประดิษฐ์ ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง หรืออาจทบทวนเพิ่มเติมได้ตามความจำเป็นเพื่อให้มีความเหมาะสม เพียงพอ และมีประสิทธิผล

แนวทางการนำไปปฏิบัติ

คณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์ ควรรับผิดชอบในการจัดทำ ทบทวน และประเมินนโยบายและมาตรฐาน AI รวมทั้งองค์ประกอบต่าง ๆ ในนโยบายและมาตรฐานดังกล่าวด้วย การทบทวนควรครอบคลุมถึงการประเมินโอกาสในการปรับปรุงนโยบายต่าง ๆ ขององค์กรด้วย และวิธีการในการบริหารจัดการระบบ AI เพื่อให้สามารถตอบสนองต่อการเปลี่ยนแปลงด้านสภาพแวดล้อมขององค์กร สถานการณ์ทางธุรกิจ ข้อกำหนดด้านกฎหมาย หรือสภาพแวดล้อมทางเทคนิคที่มีการเปลี่ยนแปลง

3.2) การจัดการภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อกำหนดความรับผิดชอบภายในองค์กรและสนับสนุนวิธีการขององค์กรในการนำระบบไปสู่การใช้งาน การใช้งานระบบ และการบริหารจัดการระบบ AI ขององค์กร

3.2.1) บทบาทและหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับ AI (AI roles and responsibilities)

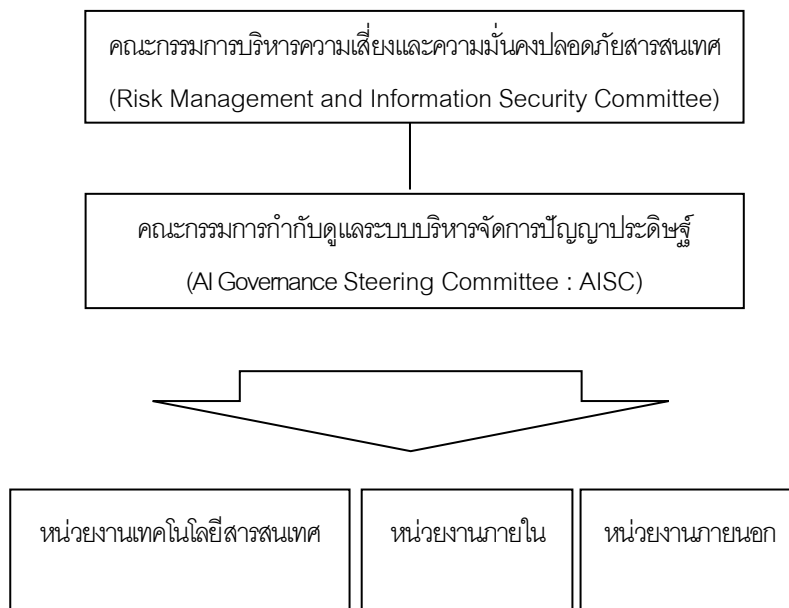
บทบาทและหน้าที่ความรับผิดชอบสำหรับ AI ต้องมีการกำหนดและมอบหมายไปยังผู้ที่เกี่ยวข้องตามความจำเป็นขององค์กร

แนวทางการนำไปปฏิบัติ

การกำหนดบทบาทและหน้าที่ความรับผิดชอบของหน่วยงานหรือผู้ที่เกี่ยวข้องมีความสำคัญต่อความรับผิดชอบที่จะเกิดขึ้นทั่วทั้งองค์กรตามบทบาทที่ได้รับที่เกี่ยวข้องกับระบบ AI ตลอดจนวงจรชีวิตของระบบ AI การมอบหมายบทบาทและหน้าที่ความรับผิดชอบควรพิจารณาจากนโยบายและมาตรฐาน วัตถุประสงค์ และความเสี่ยงที่เกี่ยวข้องกับ AI เพื่อให้มั่นใจว่าได้ครอบคลุมหน่วยงานที่เกี่ยวข้องทั้งหมด องค์กรสามารถจัดลำดับบทบาทและหน้าที่ความรับผิดชอบเหล่านั้นตามที่ต้องการ

องค์กรมีการจัดตั้งคณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์ (AI Governance Steering Committee) ดังนี้

1. ลักษณะโครงสร้างของคณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์ แสดงดังภาพด้านล่างนี้



ภาพที่ 1 แสดงโครงสร้างองค์กรของคณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์

2. คณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์ ประกอบด้วยผู้บริหารของหน่วยงานต่าง ๆ ดังนี้

(1) ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ	ประธานคณะกรรมการฯ / AIMR
(2) ผู้จัดการปัญญาประดิษฐ์	เลขานุการ / AIMA
(3) ผู้เชี่ยวชาญฝ่ายเทคโนโลยีสารสนเทศ	กรรมการ
(4) ผู้เชี่ยวชาญฝ่ายปฏิบัติการ	กรรมการ
(5) ผู้เชี่ยวชาญฝ่ายทรัพยากรบุคคล	กรรมการ
(6) ผู้เชี่ยวชาญฝ่ายพัฒนาธุรกิจ	กรรมการ
(7) ผู้เชี่ยวชาญฝ่ายการเงิน	กรรมการ
(8) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	กรรมการ

ทั้งนี้ ผู้เชี่ยวชาญแต่ละฝ่ายอาจได้รับการแต่งตั้งโดยผู้บริหารของสายงานนั้น หรืออาจเป็นผู้อำนวยการฝ่ายของสายงานนั้นโดยตำแหน่งก็ได้

คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ ได้ทำการกำหนดบทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องตามโครงสร้างของคณะกรรมการบริหารจัดการปัญญาประดิษฐ์ ดังนี้

3.2.1.1) บทบาทหน้าที่ของคณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์

- 1) กำหนดวัตถุประสงค์ของการบริหารจัดการปัญญาประดิษฐ์ขององค์กร
- 2) ตรวจสอบ ปรับปรุง กำหนด มาตรฐานการบริหารจัดการปัญญาประดิษฐ์
- 3) กำหนดเกณฑ์ในการยอมรับความเสี่ยง และผลกระทบ และ/หรือ ระดับความเสี่ยงที่ยอมรับได้ และผลกระทบที่ยอมรับได้ รวมถึงพิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญขององค์กร และรายงานต่อคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ เพื่อพิจารณานุมัติ
- 4) ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับปัญญาประดิษฐ์
- 5) วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยง และผลกระทบต่าง ๆ ขององค์กรทางด้านปัญญาประดิษฐ์
- 6) ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องในการใช้และการพัฒนาปัญญาประดิษฐ์
- 7) วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยให้เข้าใจถึงการใช้และการพัฒนาปัญญาประดิษฐ์ อย่างมีความรับผิดชอบ ถูกต้อง เหมาะสม
- 8) ให้ความสนับสนุนในการสื่อสารให้พนักงานทุกคนตระหนักถึงความสำคัญของการใช้และการพัฒนาปัญญาประดิษฐ์ อย่างมีความรับผิดชอบ และการปฏิบัติตามนโยบาย และ/หรือ มาตรฐานการบริหารจัดการปัญญาประดิษฐ์ และเอกสารต่าง ๆ ในระบบ AIMS
- 9) ให้ความสนับสนุนในการให้ความรู้แก่พนักงานและบุคคลภายนอกที่เกี่ยวข้อง ให้รับทราบและสามารถปฏิบัติตามนโยบาย และ/หรือ มาตรฐานการบริหารจัดการปัญญาประดิษฐ์และเอกสารต่าง ๆ ที่เกี่ยวข้องในระบบ AIMS รวมถึงตรวจสอบการปฏิบัติตามของพนักงานและบุคคลภายนอกที่เกี่ยวข้องอย่างเหมาะสม
- 10) รวบรวม สรุปข้อเท็จจริง ให้ความเห็น เกี่ยวกับเหตุละเมิดนโยบาย และ/หรือ มาตรฐานการบริหารจัดการปัญญาประดิษฐ์และเอกสารต่าง ๆ ที่เกี่ยวข้องในระบบ AIMS และนำเสนอข้อมูลต่อหน่วยงานที่เกี่ยวข้อง
- 11) ให้ความสนับสนุนด้านทรัพยากรที่จำเป็นในการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ AIMS
- 12) เข้าร่วมการประชุมเพื่อทบทวนการดำเนินงานของระบบ AIMS เพื่อให้มั่นใจว่าระบบ AIMS ขององค์กร มีความเหมาะสมเพียงพอ และมีประสิทธิผล รวมถึงพิจารณาโอกาสในการปรับปรุงระบบ AIMS ให้ดีขึ้นอย่างต่อเนื่อง

3.2.1.2) บทบาทหน้าที่ของ AIMR / AIMA

- 1) ดูแลการปรับปรุงแก้ไขนโยบาย มาตรฐาน และเอกสารต่าง ๆ ที่เกี่ยวข้องในระบบ AIMS ให้เหมาะสมกับการเปลี่ยนแปลงที่เกิดขึ้น สอดคล้องกับมาตรฐาน ISO/IEC 42001 และคำแนะนำที่ได้รับจาก คณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์
- 2) สื่อสารให้พนักงานทุกคนรับทราบถึงหน้าที่และความรับผิดชอบของตนในการปฏิบัติตามนโยบายและเอกสารต่าง ๆ ที่เกี่ยวข้องของระบบ AIMS
- 3) สอดส่องดูแลการปฏิบัติงานขององค์กรให้เป็นไปตามที่กำหนดไว้ในเอกสารต่าง ๆ ของระบบ AIMS
- 4) ให้คำปรึกษาและแนะนำด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและการนำนโยบายต่าง ๆ ไปใช้งาน แก่บุคลากรภายในองค์กร
- 5) จัดหาที่ปรึกษาหรือผู้เชี่ยวชาญจากภายนอกองค์กร มาให้คำปรึกษาหรือจัดฝึกอบรมในกรณีที่เป็น

- 6) ควบคุมดูแลการเปลี่ยนแปลง ต่าง ๆ ที่เกิดขึ้นในองค์กร พร้อมทั้งประสานงานให้มีการประเมิน แก้ไขและควบคุมความเสี่ยงจากการเปลี่ยนแปลงอย่างเหมาะสม
- 7) ควบคุมดูแลการวัดประสิทธิผลของกระบวนการและ Controls ในระบบ AIMS
- 8) ประสานงานและสนับสนุนการตรวจสอบภายในของระบบ AIMS (Internal AIMS Audit) ให้เป็นไปอย่างเหมาะสม
- 9) ควบคุมดูแลการดำเนินการแก้ไขและป้องกันข้อบกพร่องในระบบ AIMS รวมถึงติดตามและทบทวนประสิทธิภาพของการแก้ไขและป้องกันอย่างเหมาะสม
- 10) ประสานงานและสนับสนุนให้มีการประชุมเพื่อทบทวนการดำเนินงานของระบบ AIMS โดย AISC อย่างน้อยไตรมาสละ 1 ครั้ง และติดตามการดำเนินการตามมติที่ประชุม
- 11) รายงานผลการดำเนินงานของระบบ AIMS ซึ่งประกอบไปด้วยมาตรฐานการบริหารจัดการทั้งหมดตามที่ระบุ ต่อ AISC อย่างน้อยไตรมาสละ 1 ครั้ง
- 12) ประสานงานและหาแนวทางในการควบคุมและจัดการปัญหา ในกรณีที่เกิดเหตุละเมิดด้านปัญญาประดิษฐ์ (Incident) ขึ้นในองค์กร และรายงานต่อทีมงาน Incident Response Team หรือรายงานต่อ DPO ในกรณีที่เป็นการเหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

3.2.1.3) หน่วยงานเทคโนโลยีสารสนเทศ

จัดตั้งขึ้นเพื่อป้องกันความเสียหายขององค์กรอันเกิดจากปัญญาประดิษฐ์ เช่น การนำปัญญาประดิษฐ์ไปใช้ในทางที่ผิด เป็นต้น และทำให้การดำเนินการในส่วนที่เกี่ยวข้องกับปัญญาประดิษฐ์สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

3.2.1.3.1) ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ (Chief Technology Officer: CTO)

- (1) เป็นประธานคณะกรรมการกำกับดูแลระบบบริหารจัดการปัญญาประดิษฐ์และมีหน้าที่รับผิดชอบด้านการบริหารจัดการปัญญาประดิษฐ์และเป็นผู้ดำเนินการดำเนินงานทั้งหมดที่เกี่ยวข้องกับปัญญาประดิษฐ์ในองค์กร
- (2) กำหนดเป้าหมาย นโยบายและมาตรฐานการบริหารจัดการปัญญาประดิษฐ์ให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร
- (3) เป็นผู้เสนอแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ตลอดจนแผนการดำเนินงานทางด้านปัญญาประดิษฐ์เพื่อขอดำเนินการอนุมัติจากประธานเจ้าหน้าที่บริหารกลุ่ม (Group CEO) และประธานเจ้าหน้าที่บริหาร (CEO) และเพื่อให้มีความตระหนักในความสำคัญในเรื่องการบริหารจัดการปัญญาประดิษฐ์
- (4) วิเคราะห์และบริหารความเสี่ยงที่เกี่ยวข้องกับปัญญาประดิษฐ์ รวมถึงเป็นผู้ประเมินทางเลือกในการรับมือกับความเสี่ยงทางด้านปัญญาประดิษฐ์อย่างเหมาะสม
- (5) จัดการพัฒนานโยบายด้านการบริหารจัดการปัญญาประดิษฐ์ เพื่อให้องค์กรได้มาซึ่งเสถียรภาพของระบบปัญญาประดิษฐ์ ความถูกต้อง และการรักษาความลับของข้อมูล
- (6) บริหารจัดการใช้งานปัญญาประดิษฐ์ โดยป้องกัน ตรวจสอบการนำปัญญาประดิษฐ์ไปพัฒนาและนำไปใช้
- (7) ติดตามและรักษาความสัมพันธ์กับคู่ค้า, องค์กร หรือบุคคลภายนอก ที่มีความเกี่ยวข้องกับปัญญาประดิษฐ์ ทั้งภาครัฐและเอกชน
- (8) ตรวจสอบและอนุมัติมาตรฐานการบริหารจัดการปัญญาประดิษฐ์ รวมถึงขั้นตอน และแนวทางปฏิบัติขององค์กร เพื่อให้เหมาะสมกับความสำคัญของกระบวนการทางธุรกิจ
- (9) จัดตั้งทีมงานการบริหารจัดการปัญญาประดิษฐ์ เพื่อให้สามารถบริหารจัดการและปฏิบัติงานได้อย่างมีประสิทธิภาพ

3.2.1.3.2) ผู้จัดการปัญญาประดิษฐ์ (AI Manager)

- (1) รายงานโดยตรงกับ CTO ในการดำเนินงานทั้งหมดที่เกี่ยวข้องกับปัญญาประดิษฐ์ รวมถึง รายงานความคืบหน้าในการบริหารจัดการปัญญาประดิษฐ์ให้ CTO ทราบเป็นประจำ
- (2) ออกแบบมาตรฐานการบริหารจัดการปัญญาประดิษฐ์ รวมถึงขั้นตอนและแนวทางปฏิบัติขององค์กรเพื่อให้เหมาะสมกับความสำคัญของกระบวนการทางธุรกิจ
- (3) ทบทวนมาตรฐานและขั้นตอนทั้งหมดที่เกี่ยวข้องกับการบริหารจัดการปัญญาประดิษฐ์
- (4) เป็นที่ปรึกษาด้านปัญญาประดิษฐ์ให้กับ CTO เพื่อช่วยในการวิเคราะห์และบริหารความเสี่ยงที่เกี่ยวข้องกับปัญญาประดิษฐ์อย่างเหมาะสม รวมถึงให้ความรู้ด้านปัญญาประดิษฐ์แก่แผนกอื่น ๆ
- (5) ตรวจสอบให้แน่ใจว่ากระบวนการและการควบคุมตามที่กำหนด มีการนำไปใช้อย่างยั่งยืน
- (6) บริหารจัดการการใช้งานปัญญาประดิษฐ์ ตลอดจนวางแผนบริหารจัดการปัญญาประดิษฐ์ในด้านต่าง ๆ
- (7) ตรวจสอบและมีการติดตามการสื่อสารด้านปัญญาประดิษฐ์
- (8) เตรียมพร้อมรับสถานการณ์และเรียนรู้สิ่งใหม่เกี่ยวกับปัญญาประดิษฐ์อย่างสม่ำเสมอ
- (9) ควบคุมและบริหารทีมงานด้านปัญญาประดิษฐ์ เพื่อให้สามารถปฏิบัติงานในยามที่เกิดเหตุการณ์ที่เกี่ยวข้องกับปัญญาประดิษฐ์ขึ้นในองค์กร เช่น ข้อมูลส่วนบุคคลที่ใช้ในระบบปัญญาประดิษฐ์รั่วไหล เป็นต้น

3.2.1.3.3) ผู้ดูแลการพัฒนาปัญญาประดิษฐ์ (AI Development Team)

- (1) ดูแลงานระบบปัญญาประดิษฐ์ให้ดำเนินงานได้อย่างราบรื่น
- (2) ป้องกัน ตรวจสอบ และเฝ้าระวังระบบปัญญาประดิษฐ์ให้ทำงานอย่างถูกต้อง ไม่เกิดการรั่วไหลของข้อมูล
- (3) ปฏิบัติงานในยามที่เหตุการณ์ที่เกี่ยวข้องกับปัญญาประดิษฐ์ขึ้นในองค์กร เช่น ข้อมูลส่วนบุคคลที่ใช้ในระบบปัญญาประดิษฐ์รั่วไหล เป็นต้น
- (4) เป็นที่ปรึกษาและคอยช่วยเหลือในระหว่างการพัฒนาและในการจัดกิจกรรมการให้ความรู้ การฝึกอบรม การใช้งานปัญญาประดิษฐ์แก่ผู้ใช้

3.2.1.4) หน่วยงานภายใน

พนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับปัญญาประดิษฐ์ไม่ว่าทางใดทางหนึ่ง สามารถแบ่งได้ ดังนี้

3.2.1.4.1) หัวหน้าฝ่าย/หัวหน้าแผนก

มีหน้าที่รับผิดชอบ ดังนี้

- (1) ให้คำแนะนำและเข้าถึงความสำคัญในการใช้งานปัญญาประดิษฐ์ต่อพนักงานภายใต้การดูแล และความจำเป็นในการปกป้องข้อมูลที่เหมาะสมสำหรับการดำเนินธุรกิจ
- (2) ดำเนินการตัดสินใจทางธุรกิจให้สอดคล้องกับนโยบาย หรือ มาตรฐานการบริหารจัดการปัญญาประดิษฐ์

3.2.1.4.2) เจ้าของข้อมูล/ปัญญาประดิษฐ์

มีหน้าที่รับผิดชอบ ดังนี้

- (1) เป็นเจ้าของและควบคุมข้อมูล/ปัญญาประดิษฐ์ของตนอย่างเต็มที่ตามกฎหมาย รวมถึงข้อกำหนดในการปฏิบัติงานอื่น ๆ ที่เกี่ยวข้อง
- (2) กำหนด จัดการ ควบคุม การสร้าง การประมวลผล การเผยแพร่ และการกำจัดข้อมูล/ปัญญาประดิษฐ์

3.2.1.4.3) พนักงานองค์กร

พนักงานทุกคนขององค์กรที่มีส่วนเกี่ยวข้องกับปัญญาประดิษฐ์ไม่ว่าทางใดทางหนึ่ง มีหน้าที่รับผิดชอบ ดังนี้

- (1) ปฏิบัติตามมาตรฐานการบริหารจัดการปัญญาประดิษฐ์อย่างเคร่งครัด
- (2) รักษาความลับของข้อมูลขององค์กร ไม่นำข้อมูลความลับขององค์กรไปใช้กับปัญญาประดิษฐ์ภายนอกองค์กร และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง
- (3) รักษาความลับของข้อมูลส่วนบุคคล
- (4) รายงานเหตุการณ์หรือปัญหาในการใช้งานปัญญาประดิษฐ์ รวมถึงปัญหาทางด้านการปลอดภัยของข้อมูลเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับการใช้งานปัญญาประดิษฐ์
- (5) ใช้งานปัญญาประดิษฐ์ ข้อมูล และทรัพย์สิน AI ขององค์กรอย่างมีความรับผิดชอบ มีจริยธรรม โปร่งใส และมีความปลอดภัย รวมถึงให้ใช้งานปัญญาประดิษฐ์เฉพาะงานที่ตนเองรับผิดชอบ หรือได้รับอนุญาตเท่านั้น

โดย จะมีการหน่วยงานภายในดังต่อไปนี้ให้การสนับสนุนในส่วนงานต่างๆ ที่เกี่ยวข้องดังนี้

3.2.1.4.4) หน่วยงานฝ่ายทรัพยากรบุคคล (Human Resources) จะให้ความสนับสนุนในเรื่องต่างๆ ที่เกี่ยวกับบุคลากรขององค์กร อาทิเช่น

- (1) ให้คำแนะนำปรึกษาทางด้านนโยบายและข้อกำหนดที่เกี่ยวข้องกับการจ้างงาน การประเมินผลงาน ปัญหาด้านทรัพยากรบุคคลที่เกี่ยวข้อง รวมถึงการให้คำแนะนำเกี่ยวกับข้อมูลส่วนบุคคล
- (2) ให้การสนับสนุนด้านการบริหารจัดการเพื่อเก็บบันทึกข้อมูลที่จำเป็นเพื่อให้เป็นไปตามกฎหมายข้อบังคับและนโยบายภายในที่เกี่ยวข้องกับทรัพยากรบุคคล ซึ่งอาจมีความจำเป็นในการควบคุมการเข้าถึงระบบและการตรวจสอบการใช้งานระบบปัญญาประดิษฐ์

3.2.1.4.5) หน่วยงานฝ่ายกฎหมาย (Legal) ให้การสนับสนุนและให้คำแนะนำด้านกฎหมายเกี่ยวกับการดำเนินธุรกิจขององค์กรให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดที่เกี่ยวข้อง

3.2.1.4.6) หน่วยงานฝ่ายตรวจสอบภายใน (Internal Audit)

- (1) วางแผน ประสานงาน และดำเนินการตรวจสอบภายในสำหรับระบบบริหารจัดการปัญญาประดิษฐ์ (AIMS)
- (2) รายงานผลการตรวจสอบภายในระบบบริหารจัดการปัญญาประดิษฐ์ (AIMS) พร้อมทั้งให้คำแนะนำในการปรับปรุงแก้ไขที่เกี่ยวข้อง
- (3) ติดตามและตรวจสอบการดำเนินการแก้ไขหรือป้องกันข้อบกพร่องที่พบจากการตรวจสอบภายในระบบบริหารจัดการปัญญาประดิษฐ์ (AIMS)

3.2.1.5) หน่วยงานภายนอก

คือ บุคคลภายนอกที่เข้ามาปฏิบัติงานในองค์กรหรือทำงานให้กับองค์กร ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินปัญญาประดิษฐ์ขององค์กร เช่น ผู้ให้บริการ/ผู้จำหน่าย ระบบคู่สัญญาหรือผู้ที่ได้รับอนุญาตโดยมีหน้าที่ความรับผิดชอบ เช่นเดียวกับพนักงานขององค์กร

3.2.2) การรายงานข้อห่วงใยต่อบทบาทขององค์กรที่เกี่ยวข้องกับระบบ AI (Reporting of concerns)

องค์กรต้องกำหนดให้มีการปฏิบัติตามกระบวนการในการรายงานข้อห่วงใยต่าง ๆ ต่อบทบาทขององค์กรที่เกี่ยวข้องกับระบบ AI ตลอดจนวงจรชีวิตของระบบ รวมถึงจัดให้มีกระบวนการที่เปิดโอกาสให้ผู้ใช้งาน บุคคลที่ได้รับผลกระทบ และบุคคลภายนอกที่เกี่ยวข้อง สามารถขอให้มีการทบทวนโดยมนุษย์ และสามารถอุทธรณ์หรือโต้แย้งผลการตัดสินใจหรือผลลัพธ์ที่เกิดจาก AI ได้ตามความเหมาะสม โดยเฉพาะกรณีที่ผลลัพธ์ดังกล่าวอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญ

กลไกการรายงานข้อห่วงใยต่อบทบาทขององค์กรที่เกี่ยวข้องกับระบบ AI ควรครอบคลุมถึง

- ทางเลือกสำหรับการรายงานที่ต้องรักษาไว้เป็นความลับ และ/หรือการรายงานแบบไม่เปิดเผยตัวผู้รายงาน
- การรายงานไปยังบุคลากรขององค์กรหรือจะเป็นบุคลากรตามสัญญาจ้างก็ตาม
- การมีบุคลากรที่มีคุณสมบัติเหมาะสม
- การกำหนดเงื่อนไขของการสืบสวนสอบสวนและอำนาจในการดำเนินการต่าง ๆ
- การมีกลไกสำหรับการรายงานไปยังฝ่ายบริหารได้อย่างทันกาล
- การมีกลไกเพื่อป้องกันการแก้แค้นสำหรับทั้งบุคคลที่เกี่ยวข้องกับการรายงานและการสืบสวนสอบสวน (โดยรายงานสามารถปกปิดไว้เป็นความลับ หรือเป็นการรายงานแบบไม่เปิดเผยตัวผู้รายงานก็ได้)
- การกำหนดระยะเวลาดำเนินการที่เหมาะสมเพื่อตอบสนองต่อข้อห่วงใยที่ได้รับรายงานเข้ามา
- กระบวนการที่เป็นลายลักษณ์อักษรสำหรับผู้ใช้งาน บุคคลที่ได้รับผลกระทบ และบุคคลภายนอกที่เกี่ยวข้อง สามารถขอให้มีการทบทวนโดยมนุษย์ต่อผลการตัดสินใจหรือผลลัพธ์ที่สร้างโดย AI ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญ
- กระบวนการอุทธรณ์หรือโต้แย้งผลการตัดสินใจหรือผลลัพธ์ที่สร้างโดย AI โดยกำหนดผู้รับผิดชอบ ขั้นตอนการพิจารณา และอำนาจในการตัดสินใจอย่างชัดเจน
- อำนาจของบุคลากรที่มีคุณสมบัติเหมาะสมในการตรวจสอบ แก้ไข เปลี่ยนแปลง ยกเลิก หรือกลับคำตัดสินที่สร้างโดย AI ได้ตามความเหมาะสม
- การแจ้งผลการพิจารณาข้อร้องเรียนหรือการอุทธรณ์ให้ผู้รายงานหรือผู้ยื่นอุทธรณ์ทราบ ภายใต้ข้อจำกัดของกฎหมายและนโยบายขององค์กร
- การบันทึก ติดตาม และทบทวนข้อร้องเรียน ผลการอุทธรณ์ และการดำเนินการแก้ไข เพื่อสนับสนุนการปรับปรุงระบบ AI กระบวนการกำกับดูแล และการบริหารความเสี่ยงอย่างต่อเนื่อง

3.3) ทรัพยากรสำหรับระบบ AI (Resources for AI systems)

วัตถุประสงค์ เพื่อให้องค์กรกำหนดความรับผิดชอบด้านทรัพยากร ที่รวมถึงองค์ประกอบและทรัพยากรของระบบ AI ที่จำเป็นต้องใช้เพื่อให้สามารถจัดการกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

3.3.1) การจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากร (Resource documentation)

องค์กรต้องระบุและจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรที่จำเป็นต้องใช้สำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบ AI ตลอดจนวงจรชีวิตของระบบ รวมทั้งกิจกรรมอื่น ๆ ที่เกี่ยวข้องกับระบบ AI ขององค์กร

แนวทางการนำไปปฏิบัติ

การจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรของระบบ AI เป็นสิ่งที่มีความสำคัญเพื่อให้เข้าใจในความเสี่ยงและผลกระทบของระบบ AI (ทั้งในทางบวกและทางลบ) ที่มีต่อบุคคล กลุ่มของบุคคล หรือทั้งคู่ ตลอดจนสังคมที่เกี่ยวข้อง

ทรัพยากรของระบบ AI สามารถครอบคลุมทรัพยากรดังต่อไปนี้

- องค์ประกอบของระบบ AI
- ทรัพยากรด้านข้อมูล ได้แก่ ข้อมูลที่ใช้ในแต่ละขั้นตอนของการพัฒนาระบบ
- ทรัพยากรด้านเครื่องมือ ได้แก่ โมเดลหรืออัลกอริทึมที่ใช้งาน เครื่องมือต่างๆ
- ทรัพยากรด้านระบบคอมพิวเตอร์ ได้แก่ ฮาร์ดแวร์ที่ใช้ในการพัฒนาโมเดล สื่อบันทึกข้อมูล
- ทรัพยากรด้านบุคคล ได้แก่ บุคลากรที่มีความเชี่ยวชาญในด้านต่างๆ ครอบคลุมตลอดวงจรชีวิตของระบบ AI

ทั้งนี้ทรัพยากรอาจจะเป็นขององค์กรเอง หรือเป็นทรัพยากรที่มาจากลูกค้า หรือผู้ให้บริการภายนอกก็ได้

3.3.2) ทรัพยากรด้านข้อมูล (Data resources)

องค์กรต้องจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรด้านข้อมูลที่มีการใช้ประโยชน์โดยระบบ AI เพื่อเป็นส่วนหนึ่งของการจัดทำเอกสารด้านทรัพยากรของระบบ AI

แนวทางการนำไปปฏิบัติ

การจัดทำเอกสารที่เกี่ยวข้องกับข้อมูลที่ใช้โดยระบบ AI สามารถครอบคลุมเนื้อหา ดังนี้

- แหล่งที่มาของข้อมูล
- วันที่ซึ่งข้อมูลมีการปรับปรุงครั้งล่าสุด
- ประเภทของข้อมูล เช่น ข้อมูลที่ใช้ในการฝึกหัด ข้อมูลที่ใช้ในการทดสอบ ข้อมูลที่ใช้ในระบบจริง
- การตั้งชื่อข้อมูล
- การใช้งานข้อมูลตามที่ตั้งใจไว้
- คุณภาพของข้อมูล
- ระยะเวลาการจัดเก็บและทำลายข้อมูล
- ประเด็นด้านความอคติที่เกี่ยวข้องกับข้อมูล
- การจัดเตรียมข้อมูล

3.3.3) ทรัพยากรด้านเครื่องมือ (Tooling resources)

องค์กรต้องจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรด้านเครื่องมือที่มีการใช้งานโดยระบบ AI เพื่อเป็นส่วนหนึ่งของการจัดทำเอกสารด้านทรัพยากรของระบบ AI

แนวทางการนำไปปฏิบัติ

ทรัพยากรด้านเครื่องมือสำหรับระบบ AI และสำหรับ Machine Learning สามารถครอบคลุมทรัพยากรดังนี้

- ประเภทของอัลกอริทึมและโมเดลของ Machine Learning
- เครื่องมือหรือกระบวนการในการปรับปรุงสภาพข้อมูล

- วิธีการในการปรับปรุงอัลกอริทึมและโมเดลของ Machine Learning
- วิธีการประเมินผล
- เครื่องมือช่วยในการพัฒนาโมเดล
- ซอฟต์แวร์และฮาร์ดแวร์ที่ใช้ในการออกแบบ พัฒนาระบบ และนำระบบไปสู่การใช้งาน

3.3.4) ทรัพยากรด้านระบบและอุปกรณ์คอมพิวเตอร์ (System and computing resources)

องค์กรต้องจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรด้านระบบและอุปกรณ์คอมพิวเตอร์ที่จำเป็นต้องใช้งานโดยระบบ AI เพื่อเป็นส่วนหนึ่งของการจัดทำเอกสารด้านทรัพยากรของระบบ AI

แนวทางการนำไปปฏิบัติ

ข้อมูลที่เกี่ยวข้องกับทรัพยากรระบบและทรัพยากรคอมพิวเตอร์ของระบบ AI สามารถครอบคลุมข้อมูลดังต่อไปนี้

- ความต้องการด้านทรัพยากรของระบบ AI ที่ต้องการใช้งาน
- สถานที่ตั้งของทรัพยากรระบบและทรัพยากรคอมพิวเตอร์ของระบบ AI
- ทรัพยากรที่ใช้ในการประมวลผลของระบบ AI ซึ่งรวมถึงด้านเครือข่ายและด้านการจัดเก็บข้อมูล
- ผลกระทบของฮาร์ดแวร์สำหรับการทำงานของระบบ AI เช่น ผลกระทบที่มีต่อสิ่งแวดล้อมไม่ว่าจะโดยผ่านการใช้งานฮาร์ดแวร์ การผลิตฮาร์ดแวร์ หรือจะเป็นค่าใช้จ่ายของการใช้งานฮาร์ดแวร์ก็ตาม

3.3.5) ทรัพยากรด้านบุคคล (Human resources)

องค์กรต้องจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรด้านบุคคลและสมรรถนะที่จำเป็นของบุคคลเหล่านั้นสำหรับการพัฒนา การนำระบบไปสู่การใช้งาน การใช้งานระบบ การเปลี่ยนแปลงระบบ การบำรุงรักษาระบบ และการถ่ายโอนระบบ การถอดถอนระบบออกจากการใช้งาน การตรวจสอบความถูกต้องและเหมาะสมของระบบ ตลอดจนการบูรณาการระบบ AI เข้าเป็นส่วนหนึ่งของระบบต่าง ๆ ขององค์กร

แนวทางการนำไปปฏิบัติ

องค์กรควรจัดทำเอกสารที่เกี่ยวข้องกับทรัพยากรบุคคลและสมรรถนะของบุคคลากรดังกล่าวที่จำเป็นสำหรับการพัฒนาระบบ การนำระบบไปสู่การใช้งาน การใช้งานระบบ การดูแลระบบ การเปลี่ยนแปลงระบบ การบำรุงรักษาระบบ การโอนย้ายระบบ การถอดถอนระบบออกจากการใช้งาน การตรวจสอบความถูกต้องและเหมาะสมของระบบ ตลอดจนการบูรณาการระบบ AI เข้าเป็นส่วนหนึ่งของระบบต่าง ๆ ขององค์กร

ทรัพยากรบุคคลที่มีความจำเป็นสามารถครอบคลุมถึงทรัพยากรบุคคลดังนี้

- นักวิทยาศาสตร์ข้อมูล
- บทบาทที่เกี่ยวข้องกับการควบคุมและกำกับดูแลโดยมนุษย์
- ผู้เชี่ยวชาญที่เกี่ยวข้องกับความน่าเชื่อถือของระบบ AI เช่น ด้านความปลอดภัย ด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ด้านความเป็นส่วนตัว
- นักวิจัย ผู้ชำนาญการ และผู้เชี่ยวชาญในสาขาวิชาชีพต่าง ๆ ที่เกี่ยวข้องกับระบบ AI

3.4) การประเมินผลกระทบของระบบ AI (Assessing impacts of AI systems)

วัตถุประสงค์ เพื่อประเมินผลกระทบของระบบ AI ที่มีต่อบุคคลหรือกลุ่มของบุคคลหรือทั้งคู่และที่มีต่อสังคมที่ได้รับผลกระทบจากระบบ AI ตลอดวงจรชีวิตของระบบ

3.4.1) กระบวนการประเมินผลกระทบของระบบ AI (AI system impact assessment process)

องค์กรต้องกำหนดกระบวนการในการประเมินผลกระทบที่เป็นไปได้ของระบบ AI ที่มีต่อบุคคลหรือกลุ่มของบุคคลหรือทั้งคู่ และที่มีต่อสังคมที่อาจได้รับผลกระทบจากระบบ AI ขององค์กรตลอดวงจรชีวิตของระบบ นอกจากนี้ องค์กรต้องกำหนดให้โมเดล AI และศูนย์ข้อมูล (Data Center) ที่รองรับระบบ AI ประเภทที่มีการประมวลผลสูง (High Compute Intensity) ไม่ว่าจะเป็นขององค์กรเองหรือที่ให้บริการโดยผู้ให้บริการภายนอก ต้องคงไว้ซึ่งการมีผลกระทบทางระบบนิเวศในระดับต่ำ (Low Ecological Footprint) โดยกำหนดมาตรการที่สามารถตรวจสอบยืนยันได้ (Verifiable Measures) เพื่อลดผลกระทบทางสิ่งแวดล้อมให้น้อยที่สุด ทั้งนี้ มาตรการดังกล่าวต้องครอบคลุมถึงการวัดผลและลดการใช้พลังงานและปริมาณการปล่อยคาร์บอน การส่งเสริมเทคนิคการปรับระบบให้ทำงานอย่างเหมาะสม การกำหนดให้ใช้โครงสร้างพื้นฐานที่มีประสิทธิภาพด้านพลังงาน และการส่งเสริมการใช้พลังงานหมุนเวียนในการดำเนินงานที่เกี่ยวข้องกับระบบ AI

แนวทางการนำไปปฏิบัติ

เนื่องจากระบบ AI มีผลกระทบต่อบุคคล กลุ่มของบุคคลหรือทั้งคู่ และสังคม องค์กรที่มีการใช้งานระบบดังกล่าวควรพิจารณาจากวัตถุประสงค์ของการใช้งานระบบ AI และประเมินผลกระทบที่เป็นไปได้ของระบบ AI นั้นที่มีต่อกลุ่มคนดังกล่าว องค์กรควรพิจารณาว่าระบบ AI มีผลกระทบต่อประเด็นดังต่อไปนี้หรือไม่

- ผลกระทบด้านกฎหมาย
- ผลกระทบที่มีต่อชีวิตของบุคคล
- สุขภาพของบุคคลทางกายภาพ หรือทางด้านจิตใจ
- สิทธิของมนุษย์
- สังคม

ขั้นตอนปฏิบัติในการประเมินผลกระทบควรครอบคลุมถึง

- สถานการณ์ที่ต้องมีการประเมินผลกระทบ ที่ครอบคลุมถึง
 - วัตถุประสงค์และบริบทการใช้งาน AI หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อวัตถุประสงค์และบริบทการใช้งาน
 - ความซับซ้อนของเทคโนโลยี AI และระดับความอัตโนมัติของระบบ AI ที่ใช้งาน หรือการเปลี่ยนแปลงที่มีนัยสำคัญต่อเทคโนโลยี
 - ความอ่อนไหวของประเภทและแหล่งของข้อมูลที่ระบบ AI ใช้ในการประมวลผล หรือการเปลี่ยนแปลงที่มีนัยสำคัญต่อประเภทและแหล่งของข้อมูลดังกล่าว
- องค์กรประกอบของกระบวนการประเมินผลกระทบของระบบ AI ที่ควรครอบคลุมถึง
 - การระบุแหล่งที่มาหรือเหตุการณ์ที่สร้างผลกระทบ
 - การวิเคราะห์โอกาสเกิดขึ้นและผลกระทบ
 - การประเมินผลกระทบ
 - การจัดการกับผลกระทบ เช่น การใช้มาตรการลดความเสี่ยง
 - การจัดทำเอกสารการประเมินผลกระทบ

- การรายงานและการสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ
 - ผู้ดำเนินการประเมินผลกระทบ
 - การใช้ประโยชน์จากผลการประเมินผลกระทบ เช่น ใช้เพื่อควบคุมการออกแบบหรือใช้งานระบบ หรือเพื่อกำหนดให้มีการทบทวนและอนุมัติก่อนการใช้งาน
 - บุคคลและสังคมที่เป็นไปได้ว่าจะได้รับผลกระทบ

การประเมินผลกระทบสามารถนำประเด็นเหล่านี้มาประกอบการพิจารณา เช่น ข้อมูลที่ใช้ในการพัฒนาระบบ AI เทคโนโลยีที่ระบบ AI ใช้งาน ฟังก์ชันการทำงานของระบบ

3.4.2) การจัดทำเอกสารการประเมินผลกระทบของระบบ AI (Documentation of AI system impact assessments)

องค์กรต้องมีการจัดทำเอกสารผลการประเมินผลกระทบของระบบ AI และจัดเก็บเอกสารไว้ตามระยะเวลาที่องค์กรกำหนด

แนวทางการนำไปปฏิบัติ

เอกสารการประเมินผลกระทบของระบบ AI ควรมีการสื่อสารไปยังผู้ใช้งานและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง การประเมินผลกระทบของระบบ AI ควรมีการจัดเก็บไว้ตามระยะเวลาที่กำหนดและมีการปรับปรุงตามความจำเป็น สำหรับช่วงระยะเวลาของการจัดเก็บเอกสารการประเมินผลกระทบ ให้เป็นไปตามนโยบายการจัดเก็บเอกสารขององค์กร หรือตามที่ข้อกำหนดของกฎหมาย หรือข้อกำหนดอื่น ๆ ที่องค์กรต้องปฏิบัติ ตามหัวข้อดังต่อไปนี้ องค์กรควรพิจารณาจัดทำเป็นเอกสารไว้

- วัตถุประสงค์ของการใช้งานระบบ AI
- การใช้ผิดวัตถุประสงค์ของระบบ AI ที่คาดการณ์ว่ามีโอกาสจะเกิดขึ้น
- ผลกระทบทั้งทางบวกและทางลบของระบบ AI ที่มีต่อบุคคล กลุ่มของบุคคล หรือทั้งคู่ และสังคม
- ความล้มเหลวที่สามารถคาดการณ์ได้ ผลกระทบที่เป็นไปได้ของความล้มเหลวดังกล่าว และมาตรการที่จำเป็นต้องใช้เพื่อลดผลกระทบ
- กลุ่มของบุคคลประเภทต่าง ๆ ที่เกี่ยวข้องที่ระบบ AI มีการใช้งานกับกลุ่มของบุคคลเหล่านี้
- ความซับซ้อนของระบบ AI
- บทบาทของมนุษย์ที่เกี่ยวข้องกับระบบ ซึ่งรวมถึงการควบคุมและกำกับดูแลโดยมนุษย์
- กระบวนการและเครื่องมือที่จำเป็นเพื่อหลีกเลี่ยงผลกระทบในทางลบ
- การมีทักษะที่หลากหลายของบุคลากร

3.4.3) การประเมินผลกระทบของระบบ AI ต่อบุคคลหรือกลุ่มของบุคคล (Assessing AI system impact on individuals or groups of individuals)

องค์กรต้องประเมินและจัดทำเอกสารการประเมินผลกระทบที่เป็นไปได้ของระบบ AI ที่มีต่อบุคคลหรือกลุ่มของบุคคล ตลอดจนวงจรชีวิตของระบบนั้น เป็นประจำ

แนวทางการนำไปปฏิบัติ

เมื่อมีการประเมินผลกระทบที่มีต่อบุคคล หรือกลุ่มของบุคคล หรือทั้งคู่ และสังคม องค์กรต้องพิจารณาหลักการการกำกับดูแล นโยบาย และวัตถุประสงค์ของ AI ขององค์กร

บุคคลที่มีการใช้งานระบบ AI หรือข้อมูลส่วนบุคคลของบุคคลเหล่านี้มีการประมวลผลโดยระบบ AI อาจมีความคาดหวังต่อความน่าเชื่อถือของระบบ AI ดังกล่าว โดยเฉพาะอย่างยิ่งการป้องกันที่เป็นพิเศษสำหรับกลุ่มบุคคลเหล่านี้ เช่น เด็ก ผู้พิการ ผู้สูงอายุ ควรจะได้มีการพิจารณาดำเนินการ องค์กรต้องพิจารณา และประเมินความต้องการและความคาดหวังเหล่านี้และดำเนินการตามความต้องการดังกล่าว เพื่อเป็นส่วนหนึ่งของการประเมินผลกระทบของระบบ AI

การประเมินผลกระทบสามารถครอบคลุมถึงแต่ละด้านต่าง ๆ ดังต่อไปนี้

- ความยุติธรรมหรือความเที่ยงธรรม
- ความรับผิดชอบ
- ความโปร่งใสและความสามารถในการที่จะอธิบายการทำงานของระบบได้
- ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ และความเป็นส่วนตัว
- ความปลอดภัยและสุขภาพ
- ผลกระทบด้านการเงิน
- ความสามารถในการเข้าถึง
- สิทธิของมนุษย์

3.4.4) การประเมินผลกระทบของระบบ AI ต่อสังคม (Assessing societal impacts of AI systems)

องค์กรต้องประเมินและจัดทำเอกสารการประเมินผลกระทบที่เป็นไปได้ของระบบ AI ที่มีต่อสังคมตลอดวงจรชีวิตของระบบนั้น เป็นประจำ

แนวทางการนำไปปฏิบัติ

ผลกระทบที่มีต่อสังคมสามารถมีความหลากหลายขึ้นอยู่กับบริบทและประเภทของระบบ AI ที่องค์กรมีการใช้งาน ผลกระทบของระบบ AI อาจจะมีทั้งด้านที่เป็นประโยชน์และด้านที่เป็นอันตราย

ตัวอย่างของผลกระทบเหล่านี้ครอบคลุมถึง

- ความยั่งยืนของสิ่งแวดล้อม เช่น ผลกระทบที่มีต่อทรัพยากรตามธรรมชาติ การปล่อยก๊าซเรือนกระจก
- เศรษฐกิจ ที่รวมถึงการเข้าถึงบริการด้านการเงิน โอกาสการจ้างงาน ภาษี
- การปกครองประเทศ ที่รวมถึงกระบวนการด้านกฎหมาย การสื่อสารข้อมูลหลอกลวงเพื่อหวังผลทางการเมือง ความมั่นคงปลอดภัยระดับประเทศ ระบบศาลยุติธรรมคดีอาญา
- สุขภาพและความปลอดภัย ที่รวมถึงการเข้าถึงบริการด้านสุขภาพ การวินิจฉัยและการรักษาโรค อันตรายทั้งทางกายภาพและทางจิตใจ
- มาตรฐาน ขนบธรรมเนียมประเพณี วัฒนธรรม และค่านิยม ที่รวมถึงข้อมูลหลอกลวงหรือข้อมูลอันเป็นเท็จ (ที่ถูกสร้างขึ้นมาโดยผู้ไม่ประสงค์ดี) ที่จะนำสู่อคติหรืออันตรายต่าง ๆ ที่เกิดขึ้นกับบุคคล กลุ่มของบุคคล หรือทั้งคู่ และสังคม

ในกรณีที่โครงการหรือเครื่องมือ AI มีวัตถุประสงค์เพื่อสร้างผลกระทบต่อสังคมหรือสนับสนุนผลลัพธ์ด้านความยั่งยืน องค์กรควรกำหนดวัตถุประสงค์และตัวชี้วัดด้านความยั่งยืนที่สามารถวัดผลได้ ประเมินทั้งผลกระทบเชิงบวกและเชิงลบที่เกิดจากการใช้ AI ติดตามผลการดำเนินงานเป็นระยะ และนำผลการประเมินไปใช้ในการปรับปรุงระบบ AI โครงการด้านความยั่งยืน และการตัดสินใจขององค์กร รวมถึงรายงานผลลัพธ์ดังกล่าวต่อผู้บริหารและผู้มีส่วนได้ส่วนเสียตามความเหมาะสม

3.5) วงจรชีวิตของระบบ AI (AI system life cycle)

3.5.1) แนวทางการบริหารจัดการสำหรับการพัฒนาระบบ AI (Management guidance for AI system development)

วัตถุประสงค์ เพื่อให้มีการระบุและจัดทำเอกสารสำหรับวัตถุประสงค์และมีการดำเนินกระบวนการในการออกแบบและพัฒนาระบบ AI อย่างมีความรับผิดชอบ

หมายเหตุ : วิธีปฏิบัติขององค์กรอย่างมีความรับผิดชอบ (Responsible approach) ครอบคลุมถึงการดำเนินการต่าง ๆ ที่คำนึงถึงความเสี่ยงและผลกระทบที่ผู้มีส่วนได้ส่วนเสียกับระบบ AI จะได้รับผลกระทบเหล่านั้น องค์กรจึงต้องแสดงความรับผิดชอบต่อต่าง ๆ เพื่อป้องกันความเสี่ยงที่จะเกิดขึ้นกับผู้มีส่วนได้ส่วนเสียเหล่านั้น โดยดำเนินการต่างๆ ตามความเหมาะสม โดยพื้นฐานแล้ววิธีปฏิบัตินี้จะพิจารณาจากการกำหนดวัตถุประสงค์ของระบบ AI การกำหนดความต้องการด้านระบบ การวิเคราะห์และออกแบบระบบ การพัฒนาระบบ การนำระบบไปสู่การใช้งาน การใช้งานระบบ การเฝ้าระวังและติดตามการทำงานของระบบ และการบำรุงรักษาระบบ โดยทุกขั้นตอนดังกล่าวต้องคำนึงถึงความเสี่ยงและผลกระทบที่จะเกิดขึ้นต่อผู้มีส่วนได้ส่วนเสีย

3.5.1.1) วัตถุประสงค์สำหรับการพัฒนาระบบ AI อย่างมีความรับผิดชอบ (Objectives for responsible development of AI system)

องค์กรต้องระบุและจัดทำเอกสารสำหรับวัตถุประสงค์เพื่อให้แนวทางในการพัฒนาระบบ AI อย่างมีความรับผิดชอบ ใช้วัตถุประสงค์ดังกล่าวเพื่อประกอบการพิจารณาพัฒนาระบบ และกำหนดมาตรการเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวตลอดวงจรชีวิตของระบบ AI

แนวทางการนำไปปฏิบัติ

องค์กรต้องกำหนดวัตถุประสงค์ (ดูในข้อ 3.5.2) ที่มีผลต่อกระบวนการออกแบบและพัฒนาระบบ AI ประเด็นดังนี้สามารถนำมากำหนดเป็นวัตถุประสงค์ของการพัฒนาระบบ AI ได้

- ความยุติธรรมหรือความเที่ยงธรรม
- ความรับผิดชอบ
- ความโปร่งใส และความสามารถในการที่จะอธิบายการทำงานของระบบได้
- ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ และความเป็นส่วนตัว
- ความปลอดภัยและสุขภาพ
- ผลกระทบด้านการเงิน
- ความสามารถในการเข้าถึง
- สิทธิของมนุษย์

ถ้าองค์กรกำหนดประเด็นดังกล่าวเป็นวัตถุประสงค์ของการพัฒนาระบบ AI แล้ว ในทุกขั้นตอนของกระบวนการพัฒนาระบบ เช่น การกำหนดความต้องการของระบบ การจัดหาข้อมูลสำหรับระบบ การปรับสภาพของข้อมูล การฝึกอบรมโมเดลของระบบ การตรวจสอบความถูกต้องในการทำงานของระบบ เป็นต้น องค์กรต้องพิจารณาดำเนินการโดยกำหนดมาตรการต่าง ๆ ที่จำเป็น เพื่อให้บรรลุวัตถุประสงค์ที่ได้กำหนดไว้นั้น

3.5.1.2) กระบวนการสำหรับการออกแบบและพัฒนาระบบ AI อย่างมีความรับผิดชอบ (Processes for responsible AI system design and development)

องค์กรต้องกำหนดและจัดทำเอกสารด้านกระบวนการสำหรับการออกแบบและพัฒนาระบบ AI อย่างมีความรับผิดชอบ แนวทางการนำไปปฏิบัติ

กระบวนการพัฒนาระบบอย่างมีความรับผิดชอบควรครอบคลุมประเด็นดังต่อไปนี้

- ขั้นตอนแต่ละขั้นตอนในกระบวนการพัฒนาที่มีลักษณะเป็นวงจรการพัฒนาระบบ
- ขั้นตอนการทดสอบระบบ ที่รวมถึงข้อกำหนดในการทดสอบและวิธีการที่ใช้ในการทดสอบ
- การควบคุมและกำกับดูแลโดยมนุษย์ ที่รวมถึงกระบวนการและเครื่องมือที่จำเป็นต้องใช้ โดยเฉพาะอย่างยิ่งเมื่อระบบ AI นั้นสามารถมีผลกระทบต่อบุคคล
- ขั้นตอนการประเมินผลกระทบ
- ขั้นตอนการฝึกหัดระบบและความคาดหวัง ซึ่งรวมถึงข้อมูลใดที่ควรนำมาใช้ในการฝึกหัด การพิจารณาและอนุมัติข้อมูลที่มาจากผู้ให้บริการภายนอก
- ความเชี่ยวชาญเฉพาะทางที่จำเป็นต้องมี
- การฝึกอบรมผู้พัฒนาระบบ AI
- เกณฑ์การนำระบบไปสู่การใช้งาน
- การอนุมัติและการลงนามรับรองในแต่ละขั้นตอนของการพัฒนาระบบ
- การบริหารจัดการการเปลี่ยนแปลงระบบ

3.5.2) วงจรชีวิตของระบบ AI (AI system life cycle)

วัตถุประสงค์ เพื่อให้มีการกำหนดเกณฑ์และความต้องการของแต่ละขั้นตอนในวงจรชีวิตของระบบ AI

3.5.2.1) การกำหนดความต้องการด้านระบบ (AI system requirements and specification)

องค์กรต้องระบุและจัดทำเอกสารความต้องการด้านระบบ AI ทั้งที่เป็นระบบใหม่หรือเป็นการปรับปรุงจากระบบเดิมที่มีอยู่ แนวทางการนำไปปฏิบัติ

องค์กรควรจัดทำเอกสารเพื่อแสดงถึงเหตุผลและความจำเป็นของการพัฒนาระบบ AI และเป้าหมายของการพัฒนา ปัจจัยที่ควรนำมาพิจารณาและจัดทำเป็นเอกสารไว้ครอบคลุมถึง

- เหตุผลและความจำเป็นของการพัฒนาระบบ AI เช่น มาจากความต้องการทางธุรกิจ มาจากความต้องการของลูกค้า หรือเป็นนโยบายของรัฐบาล เป็นต้น
- วิธีการฝึกหัดโมเดลของระบบ
- การดำเนินการให้สอดคล้องกับข้อกำหนดที่เกี่ยวข้องกับข้อมูลของระบบ เช่น ข้อกำหนดด้านคุณภาพของข้อมูลของระบบ
- ข้อกำหนดหรือความต้องการที่เกี่ยวข้องกับระบบ AI ควรมีการกำหนดและครอบคลุมตลอดวงจรชีวิตของการพัฒนาระบบ AI นั้น ทบทวนและปรับปรุงข้อกำหนดดังกล่าวตามความจำเป็น เช่น เมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับข้อกำหนดตั้งต้นที่ได้กำหนดไว้

3.5.2.2) การจัดทำเอกสารการออกแบบและพัฒนาระบบ AI (Documentation of AI system design and development)

องค์กรต้องจัดทำเอกสารการออกแบบและพัฒนาระบบ AI โดยต้องมีความสอดคล้องกับวัตถุประสงค์ขององค์กร ความต้องการด้านระบบที่กำหนดไว้ รวมทั้งเกณฑ์ต่าง ๆ ที่กำหนดไว้ในเอกสารความต้องการด้านระบบ

แนวทางการนำไปปฏิบัติ

ทางเลือกสำหรับการออกแบบระบบ AI สามารถครอบคลุมถึง

- วิธีการเรียนรู้ของ Machine Learning ได้แก่ การเรียนรู้แบบมีผู้สอน (Supervised machine learning) และการเรียนรู้แบบไม่มีผู้สอน (Unsupervised machine learning)
- อัลกอริทึมและโมเดลของ Machine Learning ที่ใช้
- วิธีการฝึกหัดโมเดลและประเด็นด้านคุณภาพของข้อมูลที่ใช้ในการฝึกหัด
- การประเมินและการปรับปรุงโมเดล
- องค์ประกอบด้านฮาร์ดแวร์และซอฟต์แวร์
- ภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ
- ภัยคุกคามที่เฉพาะเจาะจงสำหรับระบบ AI (เช่น กรณีการโจมตีเพื่อให้ข้อมูลในระบบ AI ได้รับผลกระทบ (data poisoning attack) โดยการบันทึกข้อมูลที่ผิดปกติเข้าไปในระบบ AI อันจะส่งผลให้โมเดลของระบบ AI สร้างผลลัพธ์ที่ไม่ถูกต้อง หรือทำให้ประสิทธิภาพโดยรวมของระบบลดลง)
- User Interface ของระบบ
- วิธีการที่ผู้ใช้งานสามารถติดต่อกับระบบ
- การเชื่อมโยงระหว่างระบบ
- การโอนย้ายระบบให้ไปทำงานบนแพลตฟอร์มอื่น ๆ

ขั้นตอนการออกแบบระบบอาจมีการทบทวนและปรับปรุงการออกแบบระบบเป็นระยะ ๆ เพื่อให้ได้การออกแบบที่เหมาะสมที่สุดกับองค์กร เอกสารที่จัดทำขึ้นมาสำหรับการออกแบบระบบควรได้รับการปรับปรุงให้เป็นปัจจุบัน และควรมีข้อมูลสถาปัตยกรรมของระบบเป็นส่วนหนึ่งของการออกแบบระบบ

3.5.2.3) การประเมินและตรวจสอบความถูกต้องของระบบ AI (AI system verification and validation)

องค์กรต้องกำหนดมาตรการที่จำเป็นและจัดทำเป็นเอกสารสำหรับการประเมินและตรวจสอบความถูกต้องของระบบ AI รวมทั้งกำหนดเกณฑ์ที่เกี่ยวข้องของมาตรการเหล่านั้น

แนวทางการนำไปปฏิบัติ

มาตรการที่ใช้ในการประเมินความถูกต้องในการทำงานของระบบสามารถครอบคลุมถึง

- วิธีการและเครื่องมือที่ใช้ในการทดสอบระบบ
- การคัดเลือกข้อมูลที่ใช้ในการทดสอบระบบ
- ความครอบคลุมของข้อมูลที่ใช้ในการทดสอบระบบในขอบเขตของการใช้งานที่ต้องการ
- ข้อกำหนดด้านเกณฑ์การรับรองระบบ (เพื่อนำระบบไปสู่การใช้งาน)

องค์กรควรกำหนดและจัดทำเอกสารเกณฑ์การประเมินระบบโดยครอบคลุมถึง

- แผนการประเมินองค์ประกอบต่างๆ ของระบบ AI และแผนการประเมินทั้งระบบ AI โดยครอบคลุมถึงความเสี่ยงที่เกี่ยวข้องของระบบ ซึ่งจะมีผลกระทบต่อบุคคล หรือกลุ่มของบุคคล หรือทั้งคู่ และสังคม
- แผนการประเมินระบบสามารถพิจารณาจาก
 - ข้อกำหนดด้านความน่าเชื่อถือของระบบ ที่รวมถึงเกณฑ์การยอมรับข้อผิดพลาดที่อาจเกิดขึ้นได้
 - ข้อกำหนดด้านความปลอดภัยของระบบ ที่รวมถึงเกณฑ์การยอมรับข้อผิดพลาดที่อาจเกิดขึ้นได้
 - วัตถุประสงค์ของการพัฒนาและใช้งานระบบ AI อย่างมีความรับผิดชอบ
 - ปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการใช้งาน
 - การใช้งานระบบตามที่คาดหวังไว้
- วิธีการประเมินและตัวชี้วัดของการประเมินว่าผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการใช้งานระบบ AI สามารถตีความผลลัพธ์ของระบบได้อย่างถูกต้องหรือไม่
- เกณฑ์การยอมรับระบบกรณีที่ระบบไม่สามารถบรรลุระดับประสิทธิภาพเป้าหมายที่กำหนดไว้ และกลไกการปรับปรุงประสิทธิภาพให้ดียิ่งขึ้น

ระบบ AI ควรได้รับการประเมินเมื่อเทียบกับเกณฑ์การประเมินระบบที่กำหนดไว้นั้น

3.5.2.4) การนำระบบ AI ไปสู่การใช้งาน (AI system deployment)

องค์กรต้องจัดทำแผนการนำระบบไปสู่การใช้งานและต้องประเมินว่าข้อกำหนดหรือความต้องการที่เกี่ยวข้องกับระบบ AI มีความสอดคล้องก่อนนำระบบไปสู่การใช้งาน

แนวทางการนำไปปฏิบัติ

ระบบ AI สามารถพัฒนาในสภาพแวดล้อมหนึ่ง และนำไปใช้งานในสภาพแวดล้อมอื่น ๆ ได้ แต่องค์กรต้องพิจารณาให้ถี่ถ้วนว่าจะนำไปใช้ในสภาพแวดล้อมที่แตกต่างกัน

องค์กรควรกำหนดข้อกำหนดสำหรับการนำระบบไปสู่การใช้งาน ที่ต้องดำเนินการให้สอดคล้องก่อนที่จะปล่อยระบบไปสู่การใช้งาน ข้อกำหนดดังกล่าวครอบคลุมถึงมาตรการที่ใช้ในการประเมินความถูกต้องในการทำงานของระบบ ตัวชี้วัดด้านประสิทธิภาพ การทดสอบโดยผู้ใช้งาน และการอนุมัติและรับรองระบบโดยฝ่ายบริหาร

แผนการนำระบบไปสู่การใช้งานยังต้องพิจารณาถึงมุมมองของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง รวมทั้งผลกระทบต่อกลุ่มคนเหล่านั้น

3.5.2.5) การใช้งานและการเฝ้าระวังการทำงานของระบบ AI (AI system operation and monitoring)

องค์กรต้องกำหนดและจัดทำเอกสารที่เกี่ยวข้องกับการใช้งานระบบ AI อย่างต่อเนื่อง โดยอย่างน้อยต้องรวมถึงการเฝ้าระวังระบบและประสิทธิภาพของระบบ การซ่อมแซมระบบ การปรับปรุงระบบ และการให้การสนับสนุนระบบ

แนวทางการนำไปปฏิบัติ

กิจกรรมการใช้งานและการเฝ้าระวังการทำงานของระบบ AI สามารถครอบคลุมถึง

- การเฝ้าระวังการทำงานของระบบและประสิทธิภาพของระบบ ที่ครอบคลุมถึงการเฝ้าระวังข้อผิดพลาดและการล้มเหลวของระบบ ระบบทำงานตามที่คาดหวังของผู้มีส่วนได้ส่วนเสียหรือไม่ สัดส่วนของความสำเร็จในการแก้ไขปัญหาของระบบ ระบบทำงานบรรลุผลลัพธ์ตามที่ต้องการ ระดับความมั่นใจของระบบ ระบบทำงาน

อย่างสอดคล้องกับความต้องการของลูกค้าหรือไม่ ระบบทำงานอย่างสอดคล้องกับข้อกำหนดด้านกฎหมายที่องค์กรต้องปฏิบัติตามหรือไม่

- การเฝ้าระวังการทำงานของระบบว่ามีพัฒนาการด้านประสิทธิภาพที่ดีขึ้นหรือไม่ เช่น โดยการเรียนรู้ของ Machine Learning ซึ่งข้อมูลและผลลัพธ์จะถูกใช้ในการฝึกหัดโมเดลของ Machine Learning ต่อไป จึงทำให้ได้ประสิทธิภาพที่ดีขึ้น กรณีของการเรียนรู้อย่างต่อเนื่องนี้ องค์กรจำเป็นต้องเฝ้าระวังประสิทธิภาพของระบบเพื่อให้มั่นใจว่ายังคงเป็นไปตามเป้าหมายของการออกแบบระบบและยังทำงานอยู่กับข้อมูลได้ดีตามที่องค์กรต้องการหรือไม่ องค์กรควรกำหนดกลไกในการตรวจจับและแก้ไขการเปลี่ยนแปลงของข้อมูลหรือโมเดลที่อาจทำให้ประสิทธิภาพลดลง เช่น Data drift, Concept drift หรือการเสื่อมถอยของโมเดล AI เมื่อเวลาผ่านไป โดยต้องมีการติดตาม วิเคราะห์ แจ้งเตือน และดำเนินการปรับปรุงหรือฝึกโมเดลใหม่ตามความเหมาะสม
- การปรับปรุงหรือแก้ไขระบบเพื่อให้สามารถตอบสนองต่อข้อผิดพลาด การล้มเหลว ความไม่สอดคล้องกับ ความคาดหวังหรือความต้องการของลูกค้า และความไม่สอดคล้องกับข้อกำหนดของกฎหมายที่องค์กรต้องปฏิบัติตาม
- องค์กรควรมีกระบวนการเพื่อตอบสนองและแก้ไขประเด็นข้อผิดพลาดและการล้มเหลวที่พบดังกล่าว โดยทำการปรับปรุงหรือแก้ไขระบบเพื่อให้มีประสิทธิภาพที่ดีขึ้น สอดคล้องกับความต้องการของลูกค้า และข้อกำหนดด้านกฎหมายที่กำหนดไว้
- การปรับปรุงหรือแก้ไขระบบอันสืบเนื่องมาจากการเปลี่ยนแปลงด้านการใช้งานระบบการดำเนินงานต่าง ๆ ที่เกี่ยวข้องกับระบบ และการเปลี่ยนแปลงในฟังก์ชันการทำงานของระบบ องค์กรควรมีขั้นตอนปฏิบัติเพื่อจัดการกับการเปลี่ยนแปลงดังกล่าวที่เกิดขึ้นกับระบบ รวมทั้งสื่อสารให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบ
- การให้การสนับสนุนที่เกี่ยวข้องกับระบบที่อาจมาจากภายในหรือภายนอกองค์กร หรือทั้งคู่ ทั้งนี้ขึ้นอยู่กับความต้องการขององค์กรและวิธีการจัดหาระบบขององค์กร กระบวนการให้การสนับสนุนควรครอบคลุมถึงวิธีการที่ผู้ใช้งานสามารถติดต่อขอความช่วยเหลือ การแก้ไขปัญหาต่าง ๆ ที่เกี่ยวข้องกับระบบ ซึ่งรวมถึงระบบไม่สามารถใช้งานได้ ช่องทางการรายงานประเด็นปัญหาดังกล่าว ข้อตกลงการให้บริการและตัวชี้วัดของข้อตกลงดังกล่าว
- กรณีที่ระบบ AI กำลังถูกใช้งานเพื่อวัตถุประสงค์อื่น ๆ ที่นอกเหนือจากที่กำหนดไว้ในกรอบออกแบบและพัฒนา ระบบ หรือถูกใช้งานในวิธีการอื่นใดที่ไม่ได้คาดหวังไว้ ความเหมาะสมของการใช้งานดังกล่าวควรได้รับการพิจารณาใหม่
- ภัยคุกคามที่เฉพาะเจาะจงสำหรับระบบ AI ควรจะได้มีการระบุและบริหารจัดการ เช่น data poisoning, model stealing และ model inversion attacks

3.5.2.6) การจัดทำเอกสารทางเทคนิคของระบบ AI (AI system technical documentation)

องค์กรต้องกำหนดและจัดทำเอกสารทางเทคนิคของระบบ AI ที่จำเป็นสำหรับแต่ละกลุ่มของผู้มีส่วนได้ส่วนเสีย เช่น ผู้ใช้งาน หุ้นส่วน ผู้บังคับบัญชา และจัดเตรียมเอกสารไว้ในรูปแบบที่เหมาะสมสำหรับผู้มีส่วนได้ส่วนเสียเหล่านั้น

แนวทางการนำไปปฏิบัติ

เอกสารทางเทคนิคของระบบ AI สามารถครอบคลุมถึงเอกสาร ดังต่อไปนี้

- คำอธิบายทั่วไปที่เกี่ยวข้องกับระบบ AI ที่รวมถึงวัตถุประสงค์ของการใช้งาน
- คำสั่งหรือคู่มือการใช้งาน
- สมมติฐานทางเทคนิคที่เกี่ยวข้องกับการใช้งานระบบ เช่น สภาพแวดล้อมของการใช้งาน
- ข้อจำกัดทางเทคนิคของระบบ เช่น อัตราความผิดพลาดในการทำงานของระบบที่ยอมรับได้ ความถูกต้อง ความน่าเชื่อถือ ของระบบ เป็นต้น
- ขีดความสามารถและฟังก์ชันในการเฝ้าระวังการทำงานของระบบ

องค์ประกอบของเอกสารทางเทคนิคครอบคลุมถึง

- รายละเอียดการออกแบบระบบ
- สถาปัตยกรรมของระบบ
- ทางเลือกของการออกแบบระบบ
- มาตรการด้านคุณภาพที่ใช้ในช่วงการพัฒนาระบบ
- ข้อมูลที่ใช้งานในช่วงการพัฒนาระบบ
- มาตรการด้านคุณภาพสำหรับข้อมูลที่ใช้งาน
- กิจกรรมการบริหารจัดการ เช่น การบริหารความเสี่ยง
- เอกสารผลการประเมินความถูกต้องในการทำงานของระบบ
- การเปลี่ยนแปลงที่เกิดขึ้นกับระบบ เมื่อระบบได้เริ่มนำสู่การใช้งานแล้ว
- เอกสารการประเมินผลกระทบของระบบ

องค์กรควรจัดทำเอกสารทางเทคนิคที่เกี่ยวข้องกับการใช้งานระบบ AI อย่างมีความรับผิดชอบที่ครอบคลุมถึง

- แผนการบริหารจัดการการล้มเหลวของระบบ แผนถอยกลับ แผนการปรับปรุงหรือเปลี่ยนแปลงระบบ และแผนการแจ้งให้ลูกค้าและผู้ใช้งานได้รับทราบ
- กระบวนการเฝ้าระวังการทำงานของระบบ เพื่อให้ระบบทำงานได้ตามที่ต้องการและภายในขอบเขตที่กำหนดไว้
- ขั้นตอนปฏิบัติต่าง ๆ เพื่อสนับสนุนการทำงานของระบบ เช่น การเฝ้าระวังและทบทวนข้อมูลล็อกของระบบและอุปกรณ์ต่าง ๆ
- เอกสารกำหนดบทบาทของบุคลากรที่รับผิดชอบและดูแลการทำงานของระบบ
- เอกสารการเปลี่ยนแปลงระบบต่าง ๆ

องค์กรควรมีขั้นตอนปฏิบัติเพื่อรองรับการเปลี่ยนแปลงระบบต่าง ๆ ซึ่งรวมถึงการสื่อสารให้ผู้ใช้งานได้รับทราบ การจัดทำเอกสารทางเทคนิคควรมีการปรับปรุงให้เป็นปัจจุบันและมีความถูกต้อง เอกสารควรได้รับการอนุมัติโดยฝ่ายบริหารที่เกี่ยวข้อง

3.5.2.7) การบันทึกข้อมูลล็อกของเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบ AI (AI system recording of event logs)

องค์กรต้องกำหนดว่าในขั้นตอนใดของวงจรชีวิตของระบบ AI ที่ต้องมีการบันทึกข้อมูลล็อกของระบบ AI ไว้ โดยอย่างน้อยต้องมีการบันทึกข้อมูลล็อกสำหรับกิจกรรมการใช้งานระบบ AI ไว้

แนวทางการนำไปปฏิบัติ

องค์กรควรกำหนดให้มีการบันทึกข้อมูลล็อกของระบบ AI เพื่อรวบรวมและบันทึกเหตุการณ์ที่เกิดขึ้นกับระบบ การบันทึกข้อมูลล็อกควรครอบคลุมถึง

- การทำงานของฟังก์ชันต่าง ๆ ของระบบ AI
- ประสิทธิภาพของระบบ AI ทั้งที่อยู่ในขอบเขตของประสิทธิภาพที่ดีและประสิทธิภาพที่ไม่ดี
- ข้อมูลล็อกที่บันทึกไว้ควรครอบคลุมถึงวันและเวลาที่มีการใช้งานระบบ AI ข้อมูลของระบบที่ AI ทำงานกับข้อมูลดังกล่าว ผลลัพธ์ของการทำงานของระบบที่อยู่นอกเหนือจากการทำงานตามปกติ

ข้อมูลล็อกควรมีการจัดเก็บไว้ในระยะเวลาที่เหมาะสมต่อการใช้งาน สอดคล้องกับนโยบายการจัดเก็บข้อมูลขององค์กร และข้อกำหนดด้านกฎหมายที่เกี่ยวข้องกับการจัดเก็บข้อมูลที่องค์กรต้องปฏิบัติตาม

3.6) ข้อมูลสำหรับระบบ AI (Data for AI systems)

วัตถุประสงค์ เพื่อให้องค์กรเข้าใจในบทบาทและผลกระทบของข้อมูลในระบบ AI ในการประยุกต์ใช้ การพัฒนาระบบ การจัดให้มีหรือใช้งานระบบ AI ตลอดจนวงจรชีวิตของระบบ

3.6.1) ข้อมูลสำหรับการพัฒนาและปรับปรุงระบบ AI (Data for development and enhancement of AI system)

องค์กรต้องกำหนดและจัดทำเป็นเอกสารสำหรับกระบวนการบริหารจัดการข้อมูลที่เกี่ยวข้องกับการพัฒนาและการใช้งานระบบ AI รวมทั้งนำกระบวนการดังกล่าวไปสู่การปฏิบัติ

แนวทางการนำไปปฏิบัติ

การบริหารจัดการข้อมูลที่เกี่ยวข้องกับการพัฒนาระบบ AI สามารถครอบคลุมหัวข้อดังต่อไปนี้

- การจัดการความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลที่ใช้
- การจัดการภัยคุกคามด้านความมั่นคงและด้านความปลอดภัยไซเบอร์
- ความโปร่งใสและความสามารถในการอธิบายการทำงานของระบบ ซึ่งรวมถึงแหล่งที่มาของข้อมูล ที่สามารถอธิบายถึงความเชื่อมโยงของข้อมูลที่เป็น input ของระบบและข้อมูลผลลัพธ์ที่ได้จากระบบ
- ความครอบคลุมของข้อมูลที่ใช้ในการฝึกหัดระบบ
- ความถูกต้องและความครบถ้วนของข้อมูล

3.6.2) การจัดหาข้อมูลสำหรับระบบ AI (Acquisition of data)

องค์กรต้องกำหนดและจัดทำเอกสารแสดงรายละเอียดเกี่ยวกับการจัดหาและคัดเลือกข้อมูลที่ใช้ในระบบ AI

แนวทางการนำไปปฏิบัติ

องค์กรสามารถกำหนดประเภทของข้อมูลที่ใช้โดยระบบ AI ที่มาจากแหล่งของข้อมูลต่าง ๆ โดยขึ้นอยู่กับขอบเขตและการใช้งานระบบ AI ขององค์กร รายละเอียดของการจัดหาข้อมูลครอบคลุมถึง

- ประเภทของข้อมูลที่ใช้โดยระบบ AI
- ปริมาณของข้อมูลที่เป็นต้อง
- ข้อมูลได้มาอย่างไร (เช่น เป็นข้อมูลภายใน ข้อมูลที่ต้องจัดซื้อ ข้อมูลที่มีการแชร์กัน ข้อมูลเปิด หรือเป็นข้อมูลสังเคราะห์)
- คุณสมบัติของข้อมูล (เช่น เป็นข้อมูลที่ไม่เปลี่ยนแปลง เป็นข้อมูลประเภทสตรีม เป็นข้อมูลที่เก็บรวบรวมมาเป็นข้อมูลที่คอมพิวเตอร์สร้างขึ้น)

- ข้อมูลที่เกี่ยวข้องกับประชากร เช่น ข้อมูลประชากรในแต่ละช่วงอายุ เพศ รายได้ การศึกษา การจ้างงาน อัตราการแต่งงาน เป็นต้น
- การจัดการกับข้อมูลก่อนที่จะนำข้อมูลมาใช้งานกับองค์กร (เช่น ความสอดคล้องกับข้อกำหนดด้านความเป็นส่วนตัว ข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ เป็นต้น)
- สิทธิที่เกี่ยวข้องกับข้อมูล (เช่น สิทธิการใช้งานข้อมูลส่วนบุคคล ลิขสิทธิ์ เป็นต้น)
- คำอธิบายของข้อมูล (Metadata)
- แหล่งที่มาของข้อมูล (Data provenance)

3.6.3) คุณภาพของข้อมูลสำหรับระบบ AI (Quality of data for AI systems)

องค์กรต้องกำหนดและจัดทำเป็นเอกสารความต้องการด้านคุณภาพของข้อมูล และต้องมีการประเมินอย่างสม่ำเสมอว่าข้อมูลที่ใช้ในการพัฒนาระบบและข้อมูลที่ระบบใช้งานเป็นไปตามเอกสารความต้องการด้านคุณภาพดังกล่าว

แนวทางการนำไปปฏิบัติ

คุณภาพของข้อมูลที่ถูกใช้ในการพัฒนาและใช้งานระบบ AI มีผลกระทบอย่างมากกับความถูกต้องของผลลัพธ์ของระบบ AI มาตรฐาน ISO/IEC 25024 ได้นิยามคุณภาพของข้อมูลไว้ว่าเป็นระดับที่ซึ่งคุณสมบัติของข้อมูลมีความสอดคล้องกับความต้องการที่กำหนดไว้เมื่อข้อมูลนั้นถูกนำไปใช้ภายใต้เงื่อนไขที่กำหนด

สำหรับระบบ AI ที่ใช้การเรียนรู้แบบมีผู้สอน (Supervised machine learning) และแบบกึ่งมีผู้สอน (Semi-supervised machine learning) คุณภาพของข้อมูลที่ใช้ในการฝึกหัดระบบ ที่ใช้ในการทดสอบระบบและที่เป็นข้อมูลจริงในระบบ ต้องมีการกำหนด วัดผล และปรับปรุงในระดับที่เหมาะสม ข้อมูลที่ใช้งานต้องมีความเหมาะสมต่อวัตถุประสงค์ของการใช้งาน

องค์กรต้องพิจารณาผลกระทบของข้อมูลอดีตที่มีต่อประสิทธิภาพและความยุติธรรมของระบบและดำเนินการปรับปรุงโมเดลและข้อมูลที่นำมาใช้งานตามความจำเป็น เพื่อปรับปรุงทั้งประสิทธิภาพและความยุติธรรมให้อยู่ในระดับที่ยอมรับได้ต่อการนำไปใช้งาน

3.6.4) แหล่งที่มาของข้อมูล (Data provenance)

องค์กรต้องกำหนดและจัดทำเอกสารสำหรับกระบวนการบันทึกแหล่งที่มาของข้อมูลที่ใช้ในระบบ AI ขององค์กร ตลอดจนวงจรชีวิตของข้อมูลและของระบบ AI

แนวทางการนำไปปฏิบัติ

บันทึกของแหล่งที่มาของข้อมูลสามารถครอบคลุมถึงการสร้างข้อมูล การปรับปรุงข้อมูล การคัดลอกข้อมูล การคัดย่อข้อมูล การตรวจสอบความถูกต้องของข้อมูล และการถ่ายโอนข้อมูล รวมทั้งการแชร์ข้อมูลและการแปลงข้อมูลก็พิจารณาว่าอยู่ภายใต้เรื่องของแหล่งที่มาของข้อมูลโดยขึ้นอยู่กับปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการใช้งานข้อมูล เช่น เนื้อหาของข้อมูล บริบทการใช้งานข้อมูล และอื่น ๆ องค์กรควรพิจารณาว่าจำเป็นต้องมีมาตรการตรวจสอบแหล่งที่มาของข้อมูลอีกที่หนึ่งหรือไม่

3.6.5) การจัดเตรียมข้อมูล (Data preparation)

องค์กรต้องกำหนดและจัดทำเอกสารสำหรับเกณฑ์ที่ใช้ในการคัดเลือกข้อมูลและวิธีการที่ใช้ในการจัดเตรียมข้อมูลที่จะนำมาใช้กับระบบ AI

แนวทางการนำไปปฏิบัติ

ข้อมูลที่ใช้ในระบบ AI ปกติแล้วจำเป็นต้องมีการจัดเตรียมเพื่อให้สามารถใช้ประโยชน์ได้จากระบบ AI นั้น ข้อมูลที่ไม่ได้มีการจัดเตรียมให้เหมาะสมเป็นไปได้ว่าจะมีผลต่อการทำงานที่ผิดพลาดของระบบ AI

วิธีการที่ใช้ในการจัดเตรียมและแปลงข้อมูลเพื่อใช้ในระบบ AI ครอบคลุมถึง

- การสำรวจค่าทางสถิติของข้อมูลที่จะนำมาใช้ (Statistical exploration) เช่น การกระจายของข้อมูล (Distribution) ค่าเฉลี่ย (Mean) ค่ามัธยฐาน (Median) ค่าความเบี่ยงเบนมาตรฐาน (Standard deviation) ช่วงของค่าของข้อมูล (Range)
- การทำความสะอาดข้อมูล (Cleaning) เช่น การแก้ไขข้อมูล
- การเพิ่มเติมข้อมูลเข้าไปสำหรับข้อมูลที่ขาดหายไป (Imputation)
- การทำ Normalization กับชุดข้อมูล เช่น ชุดข้อมูลตั้งต้นที่เป็นตัวเลขต่างๆ นำมาหาร 10 ทั้งหมด เป็นต้น
- การกำหนดช่วงค่าของชุดข้อมูล เช่น ชุดข้อมูลมีค่าอยู่ระหว่าง 1-10 เป็นต้น
- การตั้งชื่อตัวแปรต่าง ๆ
- การกำหนดโค้ดของชุดข้อมูล เช่น การแปลงชุดข้อมูลที่เป็นหมวดหมู่ต่าง ๆ ให้เป็นโค้ดที่เป็นตัวเลขต่าง ๆ

ในการจัดเตรียมข้อมูลของระบบ AI องค์กรควรจัดทำเอกสารกำหนดเกณฑ์ในการคัดเลือกและวิธีการจัดเตรียมข้อมูล

3.7) ข้อมูลสำหรับผู้มีส่วนได้ส่วนเสียกับระบบ AI (Information for interested parties of AI systems)

วัตถุประสงค์ เพื่อให้มีข้อมูลที่สำคัญสำหรับผู้มีส่วนได้ส่วนเสียกับระบบ AI ขององค์กร เพื่อให้เข้าใจในความเสี่ยงและผลกระทบทั้งทางบวกและทางลบที่มีต่อองค์กรและผู้มีส่วนได้ส่วนเสีย

3.7.1) การจัดทำเอกสารของระบบและข้อมูลสำหรับผู้ใช้งาน (System documentation and information for users)

องค์กรต้องกำหนดและจัดเตรียมเอกสารและข้อมูลที่สำคัญสำหรับผู้ใช้งานระบบ AI

แนวทางการนำไปปฏิบัติ

ข้อมูลที่เกี่ยวข้องกับระบบ AI ครอบคลุมถึงรายละเอียดและคำสั่งหรือขั้นตอนการใช้งานทางเทคนิค ระบบ AI ควรมีการแจ้งข้อมูลให้ผู้ใช้งานได้รับทราบว่ากำลังติดต่อกับระบบ AI โดยขึ้นอยู่กับบริบทการใช้งาน ข้อมูลที่เป็นผลลัพธ์จากการทำงานของระบบ AI ก็ควรแจ้งให้ผู้ใช้งานได้รับทราบด้วย

ผู้ใช้งานควรได้รับการแจ้งให้ทราบถึงวัตถุประสงค์ของการใช้งานระบบ วิธีการที่ระบบทำงาน ประโยชน์ที่จะได้รับจากระบบ และอันตรายที่เกี่ยวข้อง (ถ้ามี)

เอกสารที่จัดเตรียมให้แก่ผู้มีส่วนได้ส่วนเสียแต่ละกลุ่มควรจะแยกกันตามลักษณะของการใช้งานและสิ่งที่ผู้มีส่วนได้ส่วนเสียจำเป็นต้องรู้และเข้าใจก่อนการใช้งาน

ข้อมูลที่สำคัญสำหรับผู้ใช้งานควรครอบคลุมถึง

- วัตถุประสงค์ของการใช้งานระบบ
- ผู้ใช้งานกำลังติดต่อกับระบบ AI
- วิธีการในการติดต่อกับระบบ AI
- วิธีการและเมื่อใดที่จะยกเลิกการใช้ระบบ AI หรือไม่ต้องใช้ระบบ AI
- ข้อกำหนดทางเทคนิคของระบบ ที่ครอบคลุมถึงทรัพยากรของระบบที่จำเป็นต้องใช้ ข้อจำกัดของระบบ และอายุการใช้งานของระบบ
- การควบคุมและกำกับดูแลโดยมนุษย์
- ข้อมูลเกี่ยวกับความถูกต้องและประสิทธิภาพของระบบ AI

- ข้อมูลที่เกี่ยวข้องจากการประเมินผลกระทบของระบบ AI ที่ครอบคลุมถึงประโยชน์และอันตรายที่เกี่ยวข้อง
- การปรับปรุงและการเปลี่ยนแปลงระบบ

3.7.2) การรายงานจากภายนอก (External reporting)

องค์กรต้องจัดเตรียมระบบและช่องทางที่จำเป็นสำหรับผู้มีส่วนได้ส่วนเสียเพื่อให้สามารถรายงานผลกระทบในทางลบของระบบ AI

แนวทางการนำไปปฏิบัติ

องค์กรควรกำหนดช่องทางสำหรับผู้ใช้งานหรือหน่วยงานภายนอกอื่น ๆ เพื่อรายงานผลกระทบในทางลบของระบบ AI (ที่นอกเหนือจากการรายงานประเด็นปัญหาและการล้มเหลวของระบบ AI เช่น ระบบไม่สามารถใช้งานได้)

3.7.3) การสื่อสารเหตุการณ์ผิดปกติ (Communication of incidents)

องค์กรต้องกำหนดและจัดทำเป็นเอกสารสำหรับแผนการสื่อสารเหตุการณ์ผิดปกติ เพื่อสื่อสารไปยังผู้ใช้งานระบบ AI

แนวทางการนำไปปฏิบัติ

เหตุการณ์ผิดปกติที่เกี่ยวข้องกับระบบ AI อาจเป็นเหตุการณ์เฉพาะเจาะจงกับระบบ AI ได้ หรือเป็นเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ หรือการละเมิดข้อมูลส่วนบุคคลก็ได้

องค์กรต้องทราบบทบาทและหน้าที่ของตนเองที่ต้องแจ้งให้ผู้ใช้งานและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบถึงเหตุการณ์ที่เกิดขึ้นนั้น สิ่งที่ต้องดำเนินการแจ้งครอบคลุมถึง

- ประเภทของเหตุการณ์ผิดปกติที่เกิดขึ้นที่ต้องมีการแจ้งให้ผู้เกี่ยวข้องได้รับทราบ
- ระยะเวลาที่ต้องแจ้งให้ทราบ
- ความจำเป็นในการแจ้งให้หน่วยงานผู้มีส่วนได้ส่วนเสียภายนอกได้รับทราบ เช่น หน่วยงานกำกับดูแลที่เกี่ยวข้อง
- รายละเอียดของสิ่งที่ต้องดำเนินการแจ้ง

องค์กรสามารถบูรณาการกิจกรรมการรายงานและการรับมือกับเหตุการณ์ผิดปกติเข้ากับกิจกรรมการรับมือในระดับองค์กร (ยกตัวอย่างเช่น กรณีของการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ก็จะมีกลไกการรับมือกับเหตุการณ์นี้เช่นกัน จึงต้องบูรณาการการรับมือในทั้งสองกรณีเข้าด้วยกันเป็นหนึ่งเดียว)

3.7.4) ข้อมูลสำหรับผู้มีส่วนได้ส่วนเสีย (Information for interested parties)

องค์กรต้องกำหนดและจัดทำเป็นเอกสารสำหรับภาระ หน้าที่ และข้อผูกพันขององค์กรในการรายงานข้อมูลข่าวสารต่าง ๆ ที่เกี่ยวข้องกับระบบ AI ไปยังผู้มีส่วนได้ส่วนเสีย

แนวทางการนำไปปฏิบัติ

ข้อมูลเกี่ยวกับเหตุการณ์ผิดปกติและอื่น ๆ ต้องมีการรายงานไปยังผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เช่น ลูกค้า หน่วยงานกำกับดูแล หน่วยงานผู้มีส่วนได้ส่วนเสียตามกฎหมาย เป็นต้น ภายในระยะเวลาตามที่กำหนดไว้ ข้อมูลที่ต้องมีการรายงานครอบคลุมถึง

- รายละเอียดทางเทคนิคของระบบ ที่ครอบคลุมถึงข้อมูลที่ใช้ในการฝึกหัดระบบ การทดสอบการทำงานของระบบ ทางเลือกของอัลกอริทึมที่ใช้
- ความเสี่ยงที่เกี่ยวข้องกับระบบ
- ผลการประเมินผลกระทบ
- ข้อมูลล็อกของระบบและข้อมูลอื่น ๆ ที่อยู่ในระบบ

องค์กรควรมีความเข้าใจในบทบาทและหน้าที่ความรับผิดชอบของตนเองที่ต้องมีการรายงานและแชร์ข้อมูลไปยังหน่วยงานผู้มีส่วนได้เสียที่เหมาะสม รวมทั้งขอบเขตอำนาจศาลที่เกี่ยวข้องด้วย เช่น กรณีมีเหตุการณ์ผิดปกติเกิดขึ้น อาจะกำหนดให้มีการรายงานข้อมูลที่เกี่ยวข้องไปยังหน่วยงานผู้มีส่วนได้เสียตามกฎหมาย

3.8) การใช้งานระบบ AI (Use of AI systems)

วัตถุประสงค์ เพื่อให้องค์กรมีการใช้งานระบบ AI อย่างมีความรับผิดชอบและเป็นไปตามนโยบายขององค์กรที่กำหนดไว้

3.8.1) กระบวนการสำหรับการใช้งานระบบ AI อย่างมีความรับผิดชอบ (Processes for responsible use of AI systems)

องค์กรต้องกำหนดและจัดทำเป็นเอกสารสำหรับกระบวนการใช้งานระบบ AI อย่างมีความรับผิดชอบ

แนวทางการนำไปปฏิบัติ

องค์กรอาจมีการพิจารณาใช้หรือไม่ใช้ระบบ AI หนึ่ง หรือพิจารณาว่าระบบ AI หนึ่งจะพัฒนาด้วยองค์กรเอง หรือเป็นการจ้างผู้ให้บริการภายนอกเป็นผู้พัฒนา องค์กรควรกำหนดมาตรฐานให้ชัดเจนสำหรับการพิจารณาดำเนินการดังกล่าวเพื่อให้เกิดการปฏิบัติอย่างถูกต้องและเหมาะสม

มาตรฐานควรครอบคลุมถึง

- การขออนุมัติการพัฒนาระบบ
- ค่าใช้จ่ายของการพัฒนาระบบ (ซึ่งรวมถึงค่าใช้จ่ายในการบำรุงรักษาระบบ)
- การขออนุมัติการจัดซื้อจัดจ้าง
- ข้อกำหนดด้านกฎหมายที่เกี่ยวข้อง
- การระบุความสามารถของ AI ที่ต้องมีการกำกับดูแลที่เข้มงวดยิ่งขึ้น เช่น การจดจำใบหน้า (Facial Recognition) การระบุตัวตนทางชีวมิติ (Biometric Identification) เทคโนโลยีการสอดแนม (Surveillance Technologies) การจดจำอารมณ์ (Emotion Recognition) หรือความสามารถอื่นของ AI ที่อาจส่งผลกระทบต่อ อย่างมีนัยสำคัญต่อสิทธิ ความเป็นส่วนตัว หรือเสรีภาพของบุคคล
- การเข้าถึงความสามารถ AI ที่อ่อนไหวต้องจำกัดเฉพาะบุคลากรที่ได้รับอนุญาตและมีความจำเป็นทางธุรกิจที่ ชอบด้วยเหตุผลเท่านั้น โดยบุคคลดังกล่าวจะสามารถเข้าถึง พัฒนา นำไปใช้งาน กำหนดค่า หรือควบคุม การทำงานของความสามารถ AI ที่อ่อนไหวได้

3.8.2) วัตถุประสงค์ของการใช้งานระบบ AI อย่างมีความรับผิดชอบ (Objectives for responsible use of AI system)

องค์กรต้องกำหนดและจัดทำเป็นเอกสารสำหรับวัตถุประสงค์เพื่อให้แนวทางในการใช้งานระบบ AI อย่างมีความรับผิดชอบ

แนวทางการนำไปปฏิบัติ

องค์กรมีการดำเนินงานในบริบทที่แตกต่างกัน จึงทำให้มีความคาดหวังและวัตถุประสงค์ที่เกี่ยวข้องกับการพัฒนาและใช้งานระบบ AI อย่างมีความรับผิดชอบที่แตกต่างกัน

โดยขึ้นอยู่กับบริบทขององค์กรนั้น ๆ องค์กรควรจะได้มีการระบุวัตถุประสงค์ของการพัฒนาและใช้งานระบบ AI อย่างมีความรับผิดชอบ ที่ครอบคลุมถึง

- ความยุติธรรมหรือความเที่ยงธรรม
- ความรับผิดชอบ
- ความโปร่งใส

- ความสามารถในการอธิบายการทำงานของระบบได้
- ความน่าเชื่อถือ
- ความปลอดภัย
- การบริหารความต่อเนื่องเพื่อรองรับสถานการณ์ต่าง ๆ ที่อาจทำให้เกิดการหยุดชะงักได้
- การรักษาความเป็นส่วนตัวและความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ
- ความสามารถในการเข้าถึงระบบได้

เมื่อได้มีการกำหนดวัตถุประสงค์ดังกล่าวแล้ว องค์กรควรจะได้กำหนดกลไกเพื่อดำเนินการให้สอดคล้องกับวัตถุประสงค์นั้น องค์กรควรกำหนดวัตถุประสงค์ที่เกี่ยวข้องกับการควบคุมและกำกับดูแลโดยมนุษย์ และกำหนดว่าในขั้นตอนใดของวงจรการพัฒนาระบบ การควบคุมและกำกับดูแลโดยมนุษย์ต้องเข้าไปเกี่ยวข้อง เพื่อให้มั่นใจว่าการตัดสินใจที่สำคัญจะไม่ถูกกระทำโดยระบบ AI เพียงลำพัง และบุคลากรที่ได้รับอนุญาตสามารถเข้าแทรกแซง ยกเลิก หรือหยุดการทำงานของ AI ได้เมื่อจำเป็น เช่น

- การตรวจสอบผลลัพธ์ของระบบ AI รวมทั้งการมีอำนาจในการยกเลิกผลลัพธ์หรือการตัดสินใจโดยระบบ AI
- การเฝ้าระวังประสิทธิภาพของระบบ AI ที่รวมถึงความถูกต้องของผลลัพธ์ของระบบ AI
- การรายงานข้อห่วงใยที่เกี่ยวข้องกับผลลัพธ์ของระบบ AI และผลกระทบที่จะเกิดขึ้นต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
- การรายงานข้อห่วงใยที่เกี่ยวข้องกับการเปลี่ยนแปลงด้านประสิทธิภาพของระบบ AI
- การพิจารณาว่าการตัดสินใจโดยอัตโนมัติของระบบ AI มีความเหมาะสมหรือไม่

การประเมินผลกระทบของระบบ AI สามารถให้ข้อมูลในเบื้องต้นว่าในขั้นตอนใดของวงจรการพัฒนาระบบที่ต้องมีการควบคุมและกำกับดูแลโดยมนุษย์ บุคลากรที่เกี่ยวข้องกับการควบคุมและกำกับดูแลโดยมนุษย์ควรได้รับแจ้งถึงรายงานการประเมินผลกระทบของระบบ AI บุคลากรเหล่านี้ควรมีความรู้และความเข้าใจในเอกสารต่าง ๆ ที่เกี่ยวข้องกับระบบ AI เพื่อให้การปฏิบัติหน้าที่เป็นไปตามวัตถุประสงค์ของการควบคุมและกำกับดูแลโดยมนุษย์ที่กำหนดไว้

3.8.3) การใช้งานระบบ AI ตามที่องค์กรต้องการ (Intended use of the AI system)

องค์กรต้องมีการประเมินการใช้ระบบ AI ว่าเป็นไปตามที่ต้องการหรือไม่ และสอดคล้องกับเอกสารที่เกี่ยวข้องกับระบบหรือไม่ แนวทางการนำไปปฏิบัติ

ระบบ AI ควรมีการนำสู่การใช้งานที่สอดคล้องกับคำสั่ง เอกสาร และคู่มือที่เกี่ยวข้องกับระบบ AI เมื่อพบว่าการใช้งานระบบ AI มีข้อห่วงใยเกิดขึ้น เช่น ผลลัพธ์ของระบบที่ได้มีผลกระทบต่อผู้มีส่วนได้ส่วนเสียควรมีการสื่อสารข้อมูลดังกล่าวไปยังผู้ที่เกี่ยวข้อง ซึ่งรวมถึงผู้ให้บริการภายนอกด้วย

องค์กรควรมีการจัดเก็บข้อมูลล็อกและเอกสารที่เกี่ยวข้องที่เกี่ยวข้องกับการใช้ระบบ AI เพื่อเป็นการยืนยันว่า ระบบมีการทำงานตามที่ต้องการหรือไม่ หรือใช้เป็นข้อมูลในการสื่อสารข้อห่วงใยที่พบกรณีที่ระบบทำงานไม่เป็นไปตามที่ต้องการ สำหรับระยะเวลาการจัดเก็บข้อมูลล็อกและเอกสารที่เกี่ยวข้อง ให้เป็นไปตามนโยบายการจัดเก็บข้อมูลขององค์กรและตามที่ข้อกำหนดของกฎหมายกำหนดไว้

3.9) ความสัมพันธ์กับผู้ให้บริการภายนอกและลูกค้า (Third-party and customer relationships)

วัตถุประสงค์ เพื่อให้เข้าใจถึงความรับผิดชอบขององค์กร และคงไว้ซึ่งความรับผิดชอบหลักนี้ และมีการจัดการความเสี่ยงเป็นส่วนอย่างเหมาะสมตามขั้นตอนที่ผู้ให้บริการภายนอกเข้ามาเกี่ยวข้องกับวงจรชีวิตของระบบ AI ขององค์กร

3.9.1) การกำหนดความรับผิดชอบ (Allocating responsibilities)

องค์กรต้องกำหนดความรับผิดชอบภายในวงจรชีวิตของระบบ AI ไปยังผู้ที่เกี่ยวข้องทั้งในส่วนขององค์กรเอง หุ่นยนต์ ผู้ให้บริการภายนอก และผู้ที่เกี่ยวข้องอื่น ๆ นอกจากการกำหนดบทบาทหน้าที่ตามกระบวนการแล้ว องค์กรต้องกำหนดผู้รับผิดชอบที่ชัดเจน (Accountable Owner) สำหรับผลลัพธ์ที่เกิดจากการทำงานของโมเดลหรือเครื่องมือ AI แต่ละระบบ เพื่อให้มั่นใจว่ามีบุคคลหรือหน่วยงานที่สามารถอธิบาย ตรวจสอบ และรับผิดชอบต่อผลกระทบที่เกิดจากผลลัพธ์ของระบบ AI นั้นได้

แนวทางการนำไปปฏิบัติ

ในวงจรการพัฒนาของระบบ AI องค์กรต้องกำหนดบทบาทและหน้าที่ความรับผิดชอบแยกกันให้ชัดเจน ระหว่างหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับระบบดังกล่าว เช่น หน่วยงานใดที่ให้ข้อมูลสำหรับระบบ AI หน่วยงานใดที่จัดเตรียมอัลกอริทึมและโมเดลของระบบ หน่วยงานที่พัฒนาระบบ หน่วยงานที่เป็นผู้ใช้ระบบ เป็นต้น

กรณีที่ต้องเป็นผู้ออกแบบระบบให้แก่หน่วยงานภายนอก องค์กรควรปฏิบัติตามวิธีปฏิบัติในการพัฒนาระบบอย่างมีความรับผิดชอบที่กำหนดไว้ในข้อ 3.5 องค์กรต้องจัดเตรียมเอกสารที่จำเป็นสำหรับระบบ AI นั้นให้แก่หน่วยงานภายนอกนั้นเพื่อนำไปใช้งานหรือใช้ประโยชน์ต่อยอดต่อไป

เมื่อมีการประมวลผลข้อมูลส่วนบุคคลในการใช้งาน และ/หรือ การพัฒนาระบบ AI ความรับผิดชอบต้องแยกกันระหว่างผู้ประมวลผลและผู้ควบคุมข้อมูลส่วนบุคคล เพื่อคุ้มครองความเป็นส่วนตัวของข้อมูลองค์กรสามารถปฏิบัติตามมาตรการที่กำหนดไว้ในมาตรฐาน ISO/IEC 27701 กรณีที่ต้องเป็นผู้ออกแบบระบบและผู้ควบคุมข้อมูลส่วนบุคคล และมีการแจ้งผู้ให้บริการภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลที่องค์กรควบคุมดูแลอยู่ เพื่อการใช้งาน การพัฒนา การดำเนินงาน การบำรุงรักษา หรือการสนับสนุนระบบ AI ผู้ให้บริการภายนอกนั้นจะมีบทบาทเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

3.9.2) ผู้ให้บริการภายนอก (Suppliers)

องค์กรต้องกำหนดกระบวนการที่เกี่ยวข้องกับการใช้บริการ ผลิตภัณฑ์ หรืออื่น ๆ ที่มาจากผู้ให้บริการภายนอก เพื่อให้เป็นไปตามหรือสอดคล้องกับวิธีการขององค์กรในการพัฒนาและใช้ระบบ AI อย่างมีความรับผิดชอบ

แนวทางการนำไปปฏิบัติ

องค์กรที่พัฒนาหรือใช้ระบบ AI สามารถใช้ประโยชน์จากผู้ให้บริการภายนอกได้ในลักษณะต่าง ๆ เช่น การใช้ชุดข้อมูลจากผู้ให้บริการ โมเดลหรืออัลกอริทึมของ Machine Learning องค์ประกอบอื่น ๆ ของระบบ เช่น ซอฟต์แวร์ไลบรารี

องค์กรสามารถพิจารณาผู้ให้บริการภายนอกประเภทต่าง ๆ ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอกเหล่านั้น และระดับความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการภายนอกแต่ละราย อันจะส่งผลต่อการคัดเลือกผู้ให้บริการภายนอกเหล่านั้น

องค์กรควรจัดทำเอกสารเพื่อแสดงว่าองค์ประกอบในส่วนใดของผู้ให้บริการภายนอก (เช่น ฮาร์ดแวร์ ซอฟต์แวร์ หรืออื่น ๆ) จะถูกบูรณาการเข้ากับระบบ AI ขององค์กร

เมื่อองค์กรพบว่าระบบ AI หรือองค์ประกอบของระบบ AI จากผู้ให้บริการภายนอกไม่เป็นไปตามความต้องการขององค์กร หรือสามารถส่งผลกระทบต่อบุคคล กลุ่มของบุคคล หรือทั้งคู่ และสังคม รวมทั้งไม่เป็นไปตามวิธีปฏิบัติขององค์กรอย่างมีความรับผิดชอบ องค์กรควรกำหนดให้ผู้ให้บริการภายนอกดำเนินการแก้ไข องค์กรสามารถตัดสินใจที่จะดำเนินงานกับผู้ให้บริการภายนอกเพื่อให้บรรลุวัตถุประสงค์ด้านความรับผิดชอบขององค์กรดังกล่าว

องค์กรควรกำหนดให้ผู้ให้บริการภายนอกส่งมอบเอกสารที่เกี่ยวข้องกับระบบ AI ที่มีความเหมาะสมและเพียงพอ (ดูข้อ 3.5.2.6 และ 3.7.1)

3.9.3) ลูกค้า (Customers)

องค์กรต้องประเมินว่าวิธีการขององค์กรในการพัฒนาและใช้ระบบ AI อย่างมีความรับผิดชอบมีการพิจารณาความต้องการและความคาดหวังของลูกค้าขององค์กร

แนวทางการนำไปปฏิบัติ

องค์กรต้องทำความเข้าใจความต้องการและความคาดหวังของลูกค้าเมื่อจำเป็นต้องส่งมอบผลิตภัณฑ์หรือบริการที่เกี่ยวข้องกับระบบ AI ให้แก่ลูกค้า (ซึ่งองค์กรในที่นี่จะทำหน้าที่เป็นผู้ให้บริการ)

ความต้องการและความคาดหวังดังกล่าวจะอยู่ในรูปของข้อกำหนดของผลิตภัณฑ์หรือบริการ หรือในรูปของข้อกำหนดในสัญญาจ้าง หรือข้อตกลงการใช้งาน องค์กรสามารถมีลูกค้าได้หลากหลายประเภท โดยแต่ละประเภทก็จะมีความต้องการและความคาดหวังที่แตกต่างกัน

องค์กรต้องทำความเข้าใจว่าความรับผิดชอบใดเป็นขององค์กรในฐานะผู้ให้บริการระบบ AI และความรับผิดชอบใดเป็นของลูกค้าในฐานะผู้ใช้บริการ โดยที่ยังคงต้องตอบสนองต่อความต้องการและความคาดหวังของลูกค้าที่กำหนดไว้

ยกตัวอย่างเช่น องค์กรสามารถระบุความเสี่ยงที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการโดยลูกค้า จึงเป็นความรับผิดชอบที่ต้องกำหนดแนวทางการจัดการกับความเสี่ยงดังกล่าวและแจ้งให้ลูกค้าได้รับทราบ เพื่อให้ลูกค้าลงมือปฏิบัติจัดการกับความเสี่ยงดังกล่าว

อีกตัวอย่างหนึ่งเพื่อแสดงถึงความรับผิดชอบขององค์กรในฐานะผู้ให้บริการ เมื่อระบบ AI ที่องค์กรเป็นผู้ให้บริการ มีความเหมาะสมต่อการใช้งานในขอบเขตหนึ่ง ข้อจำกัดของการใช้งานในขอบเขตดังกล่าวควรจะได้มีการแจ้งให้ลูกค้าได้รับทราบ เพื่อจะได้ระมัดระวังและใช้งานภายใต้ข้อจำกัดดังกล่าว

4) แนวทางการใช้เทคโนโลยี AI (Artificial Intelligence)

4.1) การใช้เทคโนโลยี AI สำหรับการดำเนินงานตามภารกิจขององค์กร

- 4.1.1) ผู้ใช้งานต้องทำการศึกษาข้อมูลเทคโนโลยี AI แต่ละประเภท เพื่อสร้างความเข้าใจเกี่ยวกับข้อมูลพื้นฐาน ศักยภาพ ประโยชน์ ความเสี่ยง และข้อจำกัด เพื่อให้ผู้ใช้งานสามารถประยุกต์ใช้เทคโนโลยี AI ได้อย่างเหมาะสม มีประสิทธิภาพ และสอดคล้องกับเป้าหมาย ของงานแต่ละประเภทที่ได้รับมอบหมาย
- 4.1.2) ผู้ใช้งานต้องประยุกต์ใช้เทคโนโลยี AI เพื่อช่วยสนับสนุน ในการดำเนินงานในบริบทที่กำหนด ดังต่อไปนี้
- การวิเคราะห์ข้อมูลและสร้างรายงาน
 - การเขียนชุดคำสั่งหรือโปรแกรม
 - การจัดทำร่างหนังสือหรือเอกสารต่าง ๆ เช่น บันทึกข้อความ นโยบาย หรือคำแนะนำ เป็นต้น
 - การให้คำแนะนำหรือแนวทางเบื้องต้นในการแก้ปัญหาต่าง ๆ
 - การสร้างเนื้อหาสำหรับการสื่อสารภายในองค์กร
 - การสร้างสื่อประชาสัมพันธ์
 - ดำเนินงานอื่น ๆ ที่ได้รับมอบหมายจากผู้บังคับบัญชา

ทั้งนี้ การประยุกต์ใช้เทคโนโลยี AI ต้องเป็นไปตามภารกิจ และเพื่อประโยชน์ขององค์กร เท่านั้น

4.2) ข้อห้ามในการใช้เทคโนโลยี AI

แม้ว่าเทคโนโลยี AI จะเป็นเครื่องมือที่ช่วยสนับสนุนและเพิ่มประสิทธิภาพในการดำเนินงานให้แก่ผู้ใช้งานอยู่หลาย ประการ แต่อย่างไรก็ตาม การใช้เทคโนโลยี AI จำต้องอยู่ในขอบเขตที่เหมาะสมและไม่ก่อให้เกิดความเสียหายใด ๆ ต่อบุคคล องค์กร สังคม หรือประเทศชาติ ในการนี้ องค์กรจึงกำหนดข้อห้ามสำหรับผู้ใช้งานเทคโนโลยี AI ไว้ดังนี้

- ห้ามใช้แทนการตัดสินใจของผู้ใช้งานในกรณีที่มีความเสี่ยงสูง เช่น การตัดสินใจ ทางกฎหมาย ทางการเงิน หรือการตัดสินใจที่อาจส่งผลกระทบต่อชีวิต ทรัพย์สินและสิทธิของบุคคล
- ห้ามเข้าถึง ติดตั้งใช้งาน กำหนดค่า หรือใช้งานระบบ AI ที่มีความสามารถอ่อนไหว ซึ่งรวมถึงการจดจำใบหน้า (Facial Recognition) การระบุตัวตนทางชีวมิติ (Biometric Identification) เทคโนโลยีการสอดแนม (Surveillance Technologies) หรือฟังก์ชัน AI ที่มีการใช้ข้อมูลที่มีความเสี่ยงสูง หรือข้อมูลส่วนบุคคล เว้นแต่ได้รับอนุญาตจากองค์กร เป็นการเฉพาะ และได้รับอนุมัติตามข้อกำหนดด้านกฎหมาย ความเป็นส่วนตัว ความมั่นคงปลอดภัยไซเบอร์ และการกำกับดูแล AI ที่เกี่ยวข้อง
- ห้ามใช้หรือเปิดเผยข้อมูลที่เป็นความลับขององค์กร โดยไม่ได้รับอนุมัติจากประธานเจ้าหน้าที่บริหารกลุ่ม (Group CEO) และประธานเจ้าหน้าที่บริหาร (CEO) ซึ่งข้อมูลที่เป็นความลับขององค์กรอาจรวมถึงข้อมูลภายในเอกสารสำคัญ หรือข้อมูลที่อาจส่งผลกระทบต่อการทำงานขององค์กร
- ห้ามใช้ข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือใช้ข้อมูลที่น่าจะเป็นความผิดตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่เกี่ยวข้อง

- ห้ามใช้เพื่อสร้างข้อมูลอันเป็นเท็จ หรือสร้างเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล องค์กร หรือสังคม อันอาจนำไปสู่ความเข้าใจผิด หรือสร้างความขัดแย้งในสังคม เช่น การสร้าง Deepfake การปลอมเสียงเพื่อหลอกลวง หรือการสร้างภาพวิดีโอที่ทำให้เกิดความเข้าใจผิด เป็นต้น
- ห้ามใช้ในทางที่ขัดต่อหลักธรรมาภิบาล คุณธรรม จริยธรรม ศีลธรรม หรือมีเจตนาแอบแฝงโดยไม่สุจริต
- ห้ามใช้เพื่อสร้างเนื้อหาที่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา รวมถึงการทำซ้ำ คัดลอก หรือ ดัดแปลงซึ่งเนื้อหาที่เป็นของบุคคลหรือหน่วยงานอื่นโดยไม่ได้รับอนุญาต
- ห้ามใช้เพื่อสร้างเนื้อหาที่ส่งเสริมการเหยียดเชื้อชาติ ศาสนา เพศ วัย ความพิการ หรือสถานะทางสังคม ซึ่งอาจขัดต่อกฎหมายและหลักสิทธิมนุษยชน
- ห้ามใช้ในการดำเนินการใด ๆ ที่อาจเป็นการกระทำความผิดตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง หลักเกณฑ์ หรืออื่น ๆ ที่เกี่ยวข้อง
- ห้ามใช้ในลักษณะที่ก่อให้เกิดอคติ (Bias) ต่อบุคคลหรือกลุ่มบุคคล เช่น การเลือกปฏิบัติ การตัดสินใจที่ไม่เป็นธรรม หรือการสร้างผลลัพธ์ที่มีความลำเอียงโดยไม่ตรวจสอบ หรือก่อให้เกิดการชักจูงแฝงเร้น เอาเปรียบจุดอ่อนของบุคคล หรือการให้คะแนนทางสังคม

4.3) การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล

การใช้งานเทคโนโลยี AI โดยเฉพาะอย่างยิ่งที่มีการให้บริการ แบบไม่มีค่าใช้จ่าย อาจมีความเสี่ยงที่ข้อมูลของผู้ใช้งานระบบ หรือโต้ตอบกับระบบ อาจถูกเข้าถึงหรือบันทึกและเพื่อปรับปรุงและพัฒนาประสิทธิภาพการทำงานของระบบ ดังนั้นเพื่อเป็นการป้องกันมิให้เกิดการรั่วไหลของข้อมูล การละเมิดสิทธิของบุคคล หรือก่อให้เกิดความเสียหาย ต่อบุคคล หน่วยงานภายนอก หรือบุคคลที่เกี่ยวข้อง องค์กรต้องคงไว้ซึ่งการควบคุมโดยมนุษย์ (Human-in-the-loop) เมื่อมีการใช้เทคโนโลยี AI ในการประมวลผลข้อมูลลับ (Confidential Information) หรือข้อมูลส่วนบุคคล โดยกำหนดให้มีการทบทวน กำกับดูแล แทรกแซง และอนุมัติโดยมนุษย์อย่างเหมาะสม ก่อนนำข้อมูลดังกล่าวไปใช้งานร่วมกับระบบ AI ผู้ใช้งานจึงต้องมีความระมัดระวังและต้องปฏิบัติ ดังนี้

- ห้ามนำข้อมูลภายในองค์กรที่มีชั้น “ข้อมูลลับ” (Confidential) เช่น เอกสารสัญญา เอกสารหรือหนังสือที่ประทับ “ข้อมูลลับ” (Confidential) เป็นต้น ไปใช้งานร่วมกับเทคโนโลยี AI แต่หากมีความจำเป็นต้องใช้ ต้องได้รับอนุมัติจากประธานเจ้าหน้าที่บริหารกลุ่ม (Group CEO) และประธานเจ้าหน้าที่บริหาร (CEO) ก่อนนำ “ข้อมูลลับ” (Confidential) มาใช้งานทุกกรณี
- ในกรณีที่ต้องใช้เทคโนโลยี AI ร่วมกับข้อมูลส่วนบุคคล ผู้พัฒนา และผู้ใช้งานต้องแจ้งต่อประธานเจ้าหน้าที่บริหารกลุ่ม (Group CEO) และประธานเจ้าหน้าที่บริหาร (CEO) และข้อมูลส่วนบุคคลที่จะนำมาใช้ จะต้องผ่านการยินยอมจากเจ้าของข้อมูล
- ในกรณีที่มีข้อสงสัยเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลหรือข้อกำหนดตามกฎหมาย ผู้ใช้งานต้องปรึกษาร่วมกับผู้บังคับบัญชา เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หรือเจ้าหน้าที่ที่เกี่ยวข้องก่อนดำเนินการใด ๆ

4.4) การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีพัฒนา หรือนำเทคโนโลยี AI มาใช้งาน

- ห้ามนำข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (เช่น รหัสผ่าน เป็นต้น) ไปใช้งานร่วมกับเทคโนโลยี AI
- ต้องตรวจสอบซอร์สโค้ดที่สร้างโดยเทคโนโลยี AI ก่อนนำมาใช้งาน โดยพิจารณาถึงความถูกต้องและการตรวจสอบช่องโหว่อย่างถี่ถ้วน
- หากพบเหตุการณ์ละเมิดความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศที่เกิดจากการประยุกต์ใช้เทคโนโลยี AI ผู้ใช้งานต้องแจ้งให้ผู้บังคับบัญชาตามลำดับชั้นทราบและต้องปฏิบัติตามขั้นตอนการปฏิบัติงาน เกี่ยวกับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศโดยทันที
- การใช้งานเทคโนโลยี AI ผู้ใช้งานต้องดำเนินการให้มีความมั่นคงปลอดภัยทางไซเบอร์, ความมั่นคงปลอดภัยของระบบสารสนเทศ, ความมั่นคงปลอดภัยของข้อมูลและความมั่นคงปลอดภัยในด้านอื่น ๆ ที่เกี่ยวข้อง
- องค์กรอาจมีการตรวจสอบการใช้เทคโนโลยีสารสนเทศ AI ของผู้ใช้งานอย่างต่อเนื่องเพื่อเป็นการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศขององค์กร

4.5) การลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มบุคคล

ด้วยผลลัพธ์จากการประยุกต์ใช้เทคโนโลยี AI มีโอกาสที่อาจสร้างเนื้อหาที่มีความคิดเชิงลบ อคติหรือแบ่งแยกอันอาจถูกเผยแพร่เป็นวงกว้างและไม่สามารถควบคุมการแพร่กระจายได้โดยง่ายอาจก่อให้เกิดความเสียหายแก่ชื่อเสียงจิตใจของบุคคลเกิดอคติหรือการเลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคลดังนั้นผู้ใช้งานจึงต้องมีความระมัดระวังและปฏิบัติ ดังนี้

- ต้องตรวจสอบเนื้อหาที่สร้างโดยเทคโนโลยี AI ก่อนนำไปใช้งานหรือเผยแพร่ต่อสาธารณะเพื่อลดหรือหลีกเลี่ยงการเกิดอคติหรือการเลือกปฏิบัติอย่างไม่เป็นธรรม
- ระมัดระวังการใช้งานเทคโนโลยี AI ในการดำเนินงานที่อาจกระทบ ต่อสิทธิของบุคคลหรือกลุ่มบุคคล หรือมีผลกระทบต่อหลักความเสมอภาค และมาตรฐานด้านสิทธิมนุษยชน

4.6) หน้าที่และความรับผิดชอบ

การนำเนื้อหาที่สร้างโดยเทคโนโลยี AI มาใช้งาน อาจส่งผลกระทบต่อปัจเจกบุคคล หน่วยงาน สังคม และประเทศชาติ ทั้งโดยเจตนาหรือไม่เจตนา ซึ่งองค์กรและผู้ใช้งาน ไม่อาจปฏิเสธความรับผิดชอบต่อผลที่เกิดขึ้นจากการกระทำดังกล่าวได้ ดังนั้นผู้ใช้งานและบุคคลที่เกี่ยวข้องกับการประยุกต์ใช้เทคโนโลยี AI จึงมีหน้าที่และความรับผิดชอบ ดังนี้

- ผู้ใช้งานต้องแจ้งผู้บังคับบัญชาเกี่ยวกับวัตถุประสงค์ ขอบเขตและลักษณะของการทำงานร่วมกันระหว่างผู้ใช้งานกับเทคโนโลยี AI (AI-Human Involvement) และเมื่อมีการใช้เทคโนโลยี AI ที่นอกเหนือจากที่องค์กรกำหนดในการปฏิบัติงาน
- ผู้ใช้งานต้องปฏิบัติตามหลักเกณฑ์และวิธีการใช้งานเทคโนโลยี AI

- ตามที่กำหนดในนโยบายนี้ และตรวจสอบเนื้อหาที่สร้างโดยเทคโนโลยี AI ก่อนนำไปใช้งานหรือเผยแพร่ และต้องมีการตรวจสอบอย่างเคร่งครัด โดยเฉพาะเนื้อหาที่เกี่ยวข้องกับกฎหมาย ข้อมูลด้านการเงิน ข้อมูลอ่อนไหว ซึ่งผู้ใช้งานจำเป็นต้องพิจารณาในประเด็นดังต่อไปนี้ ประกอบด้วย
 - ความถูกต้องของเนื้อหา
 - ผลการใช้งานหรือเผยแพร่เนื้อหาที่นำไปสู่การกระทำผิดทางกฎหมาย รวมถึงการละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือทรัพย์สินทางปัญญาอื่น ๆ
 - ความเท่าเทียมและการไม่เลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล
 - การรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล
 - ผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศและความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน
 - ผลกระทบเชิงลบอื่น ๆ ที่อาจเกิดขึ้นต่อบุคคล องค์กร สังคม และประเทศชาติ
- ผู้ใช้งานต้องรายงานให้ผู้บังคับบัญชาทราบโดยทันที ในกรณีที่การประยุกต์ใช้ AI เกิดความผิดพลาดหรือพบประเด็นปัญหา ทั้งกรณีการนำเข้าข้อมูลและแสดงผลลัพธ์ ที่อาจส่งผลกระทบต่อบุคคล องค์กร สังคม และประเทศชาติ เพื่อให้สามารถดำเนินการมาตรการแก้ไขได้โดยเร็ว
- ผู้บังคับบัญชาและผู้ใช้งานต้องมีการติดตาม ทบทวน และประเมินประสิทธิภาพ ประสิทธิผลของการใช้งานเทคโนโลยี AI อย่างต่อเนื่อง เพื่อปรับปรุงวิธีการทำงาน และการเลือกใช้เทคโนโลยี AI ที่เหมาะสมกับการปฏิบัติงาน
- การนำเนื้อหาที่สร้างจากเทคโนโลยี AI มาใช้งาน ควรมีการระบุ “สร้างโดย AI” หรือ “พัฒนาโดย AI” หรือ “Powered by AI” เพื่อให้เกิดความโปร่งใส และป้องกันความเข้าใจผิดของผู้รับข้อมูล
- AISC มีหน้าที่ในการพิจารณาตรวจสอบและนำเสนอประธานเจ้าหน้าที่บริหารกลุ่ม (Group CEO) และประธานเจ้าหน้าที่บริหาร (CEO) รายการแอปพลิเคชัน หรือบริการ AI ที่อนุญาตให้ใช้งานภายในองค์กร ตามความเหมาะสมของระดับการใช้งาน

4.7) การเคารพสิทธิในทรัพย์สินทางปัญญา

- การนำเนื้อหาที่สร้างโดยเทคโนโลยี AI ไปใช้งานหรือเผยแพร่ต่อสาธารณะ ผู้ใช้งานต้องใช้แอปพลิเคชันหรือบริการของเทคโนโลยี AI ที่องค์กรประกาศกำหนดเท่านั้น
- การประยุกต์ใช้เทคโนโลยี AI ผู้ใช้งานต้องมีความระมัดระวังไม่ให้เกิด การละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือสิทธิในทรัพย์สินทางปัญญาอื่น ๆ โดยการตรวจสอบให้แน่ใจว่าเนื้อหาที่สร้างขึ้นไม่เป็นการทำซ้ำ คัดลอก ดัดแปลง หรือใช้ประโยชน์จากผลงานที่มีเจ้าของโดยไม่ได้รับอนุญาต เพื่อป้องกันการละเมิดกฎหมายและข้อพิพาทที่อาจเกิดขึ้น

4.8) การจัดฝึกอบรมให้ความรู้เกี่ยวกับการประยุกต์ใช้เทคโนโลยี AI

องค์กรต้องจัดให้มีการอบรมพนักงาน ลูกจ้าง และผู้ปฏิบัติงานขององค์กรเกี่ยวกับ การประยุกต์ใช้เทคโนโลยี AI รวมถึงแนวทางปฏิบัติที่ถูกต้อง การใช้งานอย่างมีจริยธรรม ความมั่นคงปลอดภัย ความเสี่ยง ข้อจำกัดของเทคโนโลยี และผลกระทบที่อาจเกิดขึ้น อย่างน้อยปีละ 1 ครั้ง

4.9) โทษของการไม่ปฏิบัติตาม

กรณีสำหรับพนักงาน ลูกจ้าง ผู้ปฏิบัติ หรือผู้รับจ้างขององค์กรผู้ใดไม่ปฏิบัติตามเอกสารฉบับนี้ อาจมีผลเป็นความผิด และถูกดำเนินการทางวินัยตามข้อบังคับ ระเบียบ หรือประกาศ ขององค์กร หรือตามข้อตกลงในสัญญาจ้าง ทั้งนี้ ตามแต่กรณีและความสัมพันธ์ที่ผู้ใช้งานมีต่อองค์กร และอาจได้รับโทษตามที่กำหนดในกฎหมาย กฎ ระเบียบ หรือคำสั่งที่เกี่ยวข้อง

กรณีผู้ใช้งานพบการใช้เทคโนโลยี AI ที่ไม่ถูกต้อง ไม่เหมาะสมหรือมีความเสี่ยง อันอาจก่อให้เกิดความเสียหายใด ๆ ต้องรายงานต่อผู้บังคับบัญชา หรือเจ้าหน้าที่ที่รับผิดชอบทราบโดยทันที

4.10) ตัวอย่างพฤติกรรมที่ควรทำและไม่ควรทำ (Do's & Don'ts) ของการใช้งานเทคโนโลยี AI

พฤติกรรมที่ควรทำ (Do's)	พฤติกรรมที่ไม่ควรทำ (Don'ts)
✓ ตรวจสอบความถูกต้องของข้อมูลก่อนนำไปใช้	X นำข้อมูลไปใช้ทันทีโดยไม่ได้มีการตรวจสอบความถูกต้อง
✓ ไม่นำข้อมูลที่เป็นความลับขององค์กร ไปใช้งานร่วมกับเทคโนโลยี AI	X นำข้อมูลที่เป็นความลับขององค์กรไปใช้งานร่วมกับเทคโนโลยี AI
✓ เผยแพร่ข้อมูลที่ถูกต้องและไม่บิดเบือน	X เผยแพร่ข้อมูลที่ไม่ถูกต้อง (Misinformation) หรือบิดเบือน (Disinformation)
✓ อ้างอิงแหล่งที่มาของข้อมูลเสมอ	X ไม่มีการอ้างอิงแหล่งที่มาของข้อมูล
✓ หลีกเลี่ยงการสร้างเนื้อหาที่มีอคติ หรือเลือกปฏิบัติ	X สร้างเนื้อหาที่มีอคติหรือเลือกปฏิบัติ
✓ ใช้เครื่องมือที่ได้รับอนุญาตจากองค์กร	X ใช้เครื่องมือที่ไม่ได้รับอนุญาตจากองค์กร
✓ หลีกเลี่ยงการใช้เนื้อหาที่อาจละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา	X ใช้เนื้อหาที่อาจละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
✓ ปฏิบัติตามนโยบายและแนวทางขององค์กร	X ไม่ปฏิบัติตามนโยบายและแนวทางขององค์กร
✓ หลีกเลี่ยงการใช้งานเทคโนโลยี AI ในทางที่ผิดกฎหมาย หรือขัดต่อหลักธรรมาภิบาลคุณธรรมและจริยธรรม	X ใช้งานเทคโนโลยี AI ในทางที่ผิดกฎหมายหรือขัดต่อหลักธรรมาภิบาล คุณธรรม และจริยธรรม

5) การอ้างอิงเชิงบรรทัดฐาน (Normative references)

เอกสารต่อไปนี้ถูกอ้างถึงในข้อความในลักษณะที่เนื้อหาบางส่วนหรือทั้งหมดถือเป็นข้อกำหนดของเอกสารนี้ สำหรับการอ้างอิงที่ลงวันที่ จะใช้เฉพาะฉบับที่อ้างถึงเท่านั้น สำหรับการอ้างอิงที่ไม่มีวันที่ จะใช้เอกสารอ้างอิงฉบับล่าสุด (รวมถึงการแก้ไขใด ๆ)

- ISO/IEC 22989:2022 มาตรฐานสากลที่กำหนดคำศัพท์ กรอบแนวคิด และคำจำกัดความมาตรฐานสำหรับระบบปัญญาประดิษฐ์ (AI)
- ISO/IEC 25024:2015 มาตรฐานสากลที่ว่าด้วย "การวัดคุณภาพข้อมูล" (Measurement of Data Quality) ซึ่งเป็นส่วนหนึ่งของชุดมาตรฐาน SQuaRE (System and Software Quality Requirements and Evaluation) ที่ออกแบบมาเพื่อใช้ประเมินและวัดระดับความถูกต้องของข้อมูลในระบบคอมพิวเตอร์อย่างเป็นรูปธรรม โดยใช้เป็นเกณฑ์วัดคุณภาพข้อมูลในด้านต่างๆ เช่น ความครบถ้วน (Completeness), ความถูกต้อง (Accuracy), ความสม่ำเสมอ (Consistency), และความน่าเชื่อถือ (Credibility)

6) คำศัพท์และคำจำกัดความ (Terms and definitions)

ตารางต่อไปนี้แสดงคำจำกัดความของคำสำคัญที่ใช้ในเอกสารนี้:

คำศัพท์ (Term)	คำจำกัดความ (Definition)
องค์กร	กลุ่มบริษัทดับบลิวเอชเอ
กลุ่มบริษัทดับบลิวเอชเอ (WHA Group)	หมายถึง บริษัท ดับบลิวเอชเอ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย รวมทั้งบริษัทร่วมที่บริษัทมีอำนาจควบคุมสั่งการและกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐาน และเอกสารอื่นๆ ที่เกี่ยวข้อง
ผู้มีส่วนได้เสีย	บุคคลหรือ องค์กร ที่อาจส่งผลกระทบ ได้รับผลกระทบ หรือรับรู้ว่าตนเองได้รับผลกระทบจากการตัดสินใจหรือกิจกรรม
พนักงาน	หมายถึง พนักงานประจำ พนักงานชั่วคราว พนักงานทดลองงาน พนักงานที่มีการกำหนดระยะเวลาการจ้าง พนักงานสัญญาจ้างพิเศษตามระเบียบข้อบังคับเกี่ยวกับการทำงานและสภาพการจ้างของกลุ่มบริษัทดับบลิวเอชเอ รวมทั้งพนักงานที่ได้รับการว่าจ้างผ่านบริษัทคู่สัญญา
ระบบบริหารจัดการ	ชุดขององค์ประกอบที่สัมพันธ์กันหรือมีปฏิสัมพันธ์ของ องค์กร เพื่อกำหนด นโยบาย มาตรฐานและวัตถุประสงค์ ตลอดจนกระบวนการ เพื่อให้บรรลุวัตถุประสงค์เหล่านั้น
นโยบาย	เจตนารมณ์และทิศทางขององค์กร ตามที่แสดงอย่างเป็นทางการโดยผู้บริหารระดับสูง
มาตรฐาน	เอกสาร ข้อกำหนด หลักเกณฑ์ หรือลักษณะเฉพาะที่ถูกจัดทำขึ้นโดยความเห็นชอบร่วมกัน เพื่อใช้เป็นกติกากลางในการอ้างอิงและควบคุมคุณภาพการปฏิบัติงาน กระบวนการ หรือบริการให้มีความสม่ำเสมอ มั่นคงปลอดภัย และใช้งานร่วมกันได้ ซึ่งช่วยเพิ่มความน่าเชื่อถือและลดความซ้ำซ้อน
ความเสี่ยง	ผลกระทบของความไม่แน่นอน ซึ่งอาจเกิดขึ้นได้จากหลายปัจจัย เช่น - ข้อมูลเท็จและการบิดเบือนข้อมูล: การสร้างข้อมูลเท็จที่ไม่ได้ตั้งใจให้เกิดความเข้าใจผิด (Misinformation) และข้อมูลเท็จที่จงใจให้เกิดความเข้าใจผิด (Disinformation) อาจทำให้ผู้ใช้งานเชื่อว่าข้อมูลนั้นถูกต้องและนำไปใช้งานโดยไม่พิจารณาถึงความเหมาะสมและข้อจำกัดของเทคโนโลยี - ความเป็นส่วนตัวของข้อมูล: การใช้เทคโนโลยี AI อาจส่งผลกระทบต่อความเป็นส่วนตัวของข้อมูล โดยเฉพาะเมื่อมีการใช้งานข้อมูลส่วนบุคคลที่อ่อนไหว - อคติและการเลือกปฏิบัติ: ผลลัพธ์จากการประยุกต์ใช้เทคโนโลยี AI อาจสร้างเนื้อหาที่มีความคิดเชิงลบ อคติ หรือแบ่งแยก ซึ่งอาจก่อให้เกิดความเสียหายแก่ชื่อเสียงและจิตใจของบุคคล - ความมั่นคงปลอดภัยของข้อมูล: การใช้เทคโนโลยี AI อาจทำให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล เช่น การรั่วไหลของข้อมูลส่วนบุคคล หรือการละเมิดทรัพย์สินทางปัญญา - ผลกระทบเชิงลบอื่น ๆ: การใช้เทคโนโลยี AI อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคล องค์กร สังคม และประเทศชาติ เช่น การสร้างเนื้อหาที่ไม่ถูกต้องตามข้อเท็จจริง หรือเนื้อหาที่มีความอันตรายหรือรุนแรง
AI	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้ระบบประมวลผลของคอมพิวเตอร์ หุ่นยนต์ เครื่องจักร หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ตามวัตถุประสงค์ที่มนุษย์กำหนด เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา

- END OF DOCUMENT -