นโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์

(AI Governance Policy)

Enterprise IT Governance Office

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) | 2 ซอยศูนย์วิจัย 7 ถนนเพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310

สารบัญ

นโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์

(AI Governance Policy)

องค์กรตระหนักว่าเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มีบทบาทสำคัญในการขับเคลื่อนการเปลี่ยนผ่านสู่ระบบสุขภาพดิจิทัล โดยสนับสนุนการยกระดับประสิทธิภาพการให้บริการทางการแพทย์ การวิเคราะห์ข้อมูลสุขภาพ การบริหารจัดการทรัพยากร และการสนับสนุนการตัดสินใจทางคลินิก ซึ่งสามารถช่วยยกระดับคุณภาพการดูแลรักษา ประสิทธิภาพการดำเนินงาน และผลลัพธ์ทางสุขภาพของผู้ป่วยได้อย่างมีนัยสำคัญ

อย่างไรก็ตาม การนำระบบปัญญาประดิษฐ์ มาใช้ในบริบทด้านสุขภาพเป็นการดำเนินงานที่มีความอ่อนไหวและมีความเสี่ยงสูง เนื่องจากอาจส่งผลกระทบโดยตรงต่อความปลอดภัยของผู้ป่วย ความถูกต้องของการวินิจฉัยและการรักษา จริยธรรมทางการแพทย์ ตลอดจนการคุ้มครองข้อมูลสุขภาพส่วนบุคคล นอกจากนี้ ลักษณะของระบบ AI ที่อาศัยข้อมูลจำนวนมาก การตัดสินใจอัตโนมัติ และการเปลี่ยนแปลงของระบบตามข้อมูลหรือบริบทการใช้งาน อาจก่อให้เกิดความเสี่ยงด้านความโปร่งใส ความเป็นธรรม ความเอนเอียงของข้อมูล (Bias) ความสามารถในการอธิบายผลลัพธ์ (Explainability) ความมั่นคงปลอดภัยไซเบอร์ และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ซึ่งจำเป็นต้องได้รับการกำกับดูแลและบริหารจัดการอย่างเหมาะสม รัดกุม และเป็นระบบ

ดังนั้น บริษัทจึงกำหนดนโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์ (AI Governance Policy) เพื่อใช้เป็นกรอบการกำกับดูแลและบริหารจัดการระบบ AI ในระดับองค์กร สำหรับการพัฒนา การจัดหา การนำมาใช้ และการใช้งานระบบ AI ตลอดวงจรชีวิต ทั้งนี้ องค์กรต้องนำนโยบาย กรอบการกำกับดูแล และข้อกำหนดที่บริษัทกำหนดไปประยุกต์ใช้ให้สอดคล้องกับลักษณะธุรกิจ รูปแบบการดำเนินงาน ระดับความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง เพื่อให้การดำเนินงานด้านระบบ AI เป็นไปอย่างมีประสิทธิผล โปร่งใส สามารถตรวจสอบย้อนหลังได้ และสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ ระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) หลักการใช้งานระบบ AI อย่างมีความรับผิดชอบ (Responsible AI) รวมถึงกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง

1. **วัตถุประสงค์** (Purpose)

1.1 กำหนดกรอบการกำกับดูแลและบริหารจัดการระบบ AI สำหรับการพัฒนา การจัดหา การนำมาใช้ และการใช้งานระบบ AI อย่างเป็นระบบ โปร่งใส และสอดคล้องกับยุทธศาสตร์องค์กร หลักธรรมาภิบาล ระดับความเสี่ยงที่องค์กรยอมรับได้ และข้อกำหนดที่เกี่ยวข้อง

1.2 บูรณาการการบริหารจัดการความเสี่ยงด้านระบบ AI เข้ากับกระบวนการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management: ERM) โดยกำหนดให้มีการระบุ ประเมิน ควบคุม ติดตาม และรายงานความเสี่ยงที่เกี่ยวข้องกับระบบ AI อย่างเป็นระบบ สม่ำเสมอ และสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้

1.3 ส่งเสริมการใช้ระบบ AI อย่างมีความรับผิดชอบ (Responsible AI) โปร่งใส เป็นธรรม สามารถตรวจสอบย้อนหลังได้ และสอดคล้องกับหลักจริยธรรม รวมถึงสนับสนุนการคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยสารสนเทศ สิทธิของผู้มีส่วนได้เสีย และการปฏิบัติตามกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง

1.4 สนับสนุนการสร้างคุณค่าทางธุรกิจ นวัตกรรม และการยกระดับประสิทธิภาพการดำเนินงาน ผ่านการใช้ระบบ AI อย่างเหมาะสม โดยคำนึงถึงความสมดุลระหว่างโอกาสทางธุรกิจ การบริหารจัดการความเสี่ยง การกำกับดูแลที่เหมาะสม และความยั่งยืนขององค์กร

2. ขอบเขต (Scope)

นโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์ (AI Governance Policy) ฉบับนี้ กำหนดขึ้นเพื่อใช้เป็นกรอบการกำกับดูแลและบริหารจัดการระบบ AI ทั่วทั้งองค์กร และให้มีผลบังคับใช้กับการพัฒนา การจัดหา การนำมาใช้ การบูรณาการ และการใช้งานระบบที่เข้าข่ายเป็นระบบ AI ตามหลักเกณฑ์ที่บริษัทกำหนดและอยู่ภายใต้ความรับผิดชอบขององค์กร ไม่ว่าจะดำเนินการโดยหน่วยงานภายใน หรือผ่านผู้รับจ้าง ผู้ให้บริการ ที่ปรึกษา พันธมิตรทางธุรกิจ หรือบุคคลภายนอกอื่นใดที่ดำเนินการแทนหรือในนามขององค์กร

ขอบเขตของนโยบายฉบับนี้ครอบคลุมอย่างน้อยดังต่อไปนี้

1. ระบบ AI ที่องค์กรพัฒนาเอง (In-house Development) รวมถึงแบบจำลอง (Models) เครื่องมือ แพลตฟอร์ม อัลกอริทึม ชุดข้อมูล และองค์ประกอบที่เกี่ยวข้องกับระบบ AI ที่ได้รับการออกแบบ พัฒนา ปรับแต่ง หรือดำเนินการโดยบุคลากรขององค์กรหรือผู้ที่ดำเนินการแทนองค์กร
2. ระบบ AI ที่จัดหา ใช้บริการ หรือบูรณาการจากผู้ให้บริการภายนอก (Third-party / Vendor AI Solutions) รวมถึงบริการในรูปแบบ Software as a Service (SaaS), Platform as a Service (PaaS), Application Programming Interface (API), Foundation Models, Generative AI Services หรือรูปแบบบริการอื่นที่เกี่ยวข้อง
3. การใช้งานระบบ AI เพื่อสนับสนุนกระบวนการทางธุรกิจ การให้บริการ การวิเคราะห์ข้อมูล การตัดสินใจ การปฏิบัติงานอัตโนมัติ หรือกิจกรรมอื่นใดขององค์กร โดยเฉพาะกรณีที่เกี่ยวข้องกับข้อมูลสุขภาพ ข้อมูลส่วนบุคคล ข้อมูลสำคัญขององค์กร หรือกระบวนการที่มีความเสี่ยงสูง
4. ระบบงาน กระบวนการ หรือบริการที่มีการใช้ระบบ AI เป็นองค์ประกอบสำคัญในการตัดสินใจ การให้คำแนะนำ การคาดการณ์ การจำแนกผลลัพธ์ หรือการประมวลผลข้อมูลตามหลักเกณฑ์ที่บริษัทกำหนด

สำหรับระบบปัญญาประดิษฐ์ที่มีความเสี่ยงสูง (High-Risk AI) บริษัทอาจกำหนดหลักเกณฑ์ ประเภท กรณีการใช้งาน เงื่อนไข หรือมาตรการควบคุมเพิ่มเติมสำหรับการพัฒนา จัดหา หรือการนำระบบ AI มาใช้งาน โดยองค์กรต้องดำเนินการภายใต้กระบวนการกำกับดูแล การพิจารณา และการอนุมัติตามที่บริษัทกำหนดก่อนดำเนินการ

นโยบายฉบับนี้ถือเป็นข้อกำหนดที่มีผลบังคับใช้กับคณะกรรมการ ผู้บริหาร พนักงาน และบุคลากรที่เกี่ยวข้องทุกระดับ ภายในกลุ่มธุรกิจของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) บริษัทย่อย และกิจการอื่นใดที่บริษัทมีอำนาจควบคุมการดำเนินงาน ไม่ว่าทางตรงหรือทางอ้อม (รายละเอียดตามเอกสารแนบท้าย) รวมถึง ผู้รับจ้าง ที่ปรึกษา ผู้ให้บริการ และบุคคลภายนอกอื่นที่มีส่วนเกี่ยวข้องกับการพัฒนา การจัดหา การกำกับดูแล หรือการใช้งานระบบ AI ในนามขององค์กร เว้นแต่กรณีที่มีกฎหมายหรือข้อกำหนดเฉพาะกำหนดไว้เป็นอย่างอื่น และได้รับความเห็นชอบตามกระบวนการกำกับดูแลที่องค์กรกำหนด

ทั้งนี้ ให้ใช้บังคับร่วมกับนโยบาย ระเบียบ มาตรฐาน และแนวทางปฏิบัติอื่นที่เกี่ยวข้องขององค์กร เช่น การกำกับดูแลเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล โดยในกรณีที่มีเนื้อหาที่เกี่ยวข้องหรือทับซ้อนกัน ให้ตีความและบังคับใช้ในลักษณะที่สนับสนุนกรอบการกำกับดูแล การบริหารจัดการความเสี่ยง และการปฏิบัติตามข้อกำหนดขององค์กรโดยรวมเป็นสำคัญ

3. คำจำกัดความ (Definitions)

คำศัพท์	ความหมาย
1. บริษัท	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
2. บริษัทย่อย	บริษัทที่บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) มีอำนาจควบคุมการดำเนินงาน
3. องค์กร	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย

คำศัพท์	ความหมาย
4. ปัญญาประดิษฐ์ (Artificial Intelligence : AI)	เทคโนโลยีหรือระบบคอมพิวเตอร์ที่สามารถประมวลผลข้อมูล วิเคราะห์ เรียนรู้ สร้างผลลัพธ์ หรือสนับสนุนการตัดสินใจ โดยอาศัยแบบจำลอง อัลกอริทึม เทคนิคการเรียนรู้ของเครื่อง (Machine Learning) หรือวิธีการที่มีลักษณะคล้ายคลึงกัน
5. ระบบ AI (AI System)	ระบบ ซอฟต์แวร์ แพลตฟอร์ม โมเดล หรือองค์ประกอบใด ๆ ที่ใช้เทคโนโลยีปัญญาประดิษฐ์ในการประมวลผล วิเคราะห์ คาดการณ์ สร้างเนื้อหา หรือสนับสนุนการดำเนินงานและการตัดสินใจขององค์กร
6. โมเดล AI (AI Model)	แบบจำลองทางคณิตศาสตร์ สถิติ หรือการคำนวณ ที่ได้รับการพัฒนา ฝึกสอน หรือปรับแต่ง เพื่อใช้ในการประมวลผลข้อมูล วิเคราะห์ คาดการณ์ จำแนกประเภท หรือสร้างผลลัพธ์ตามวัตถุประสงค์ที่กำหนด
7. การกำกับดูแลระบบ AI (AI Governance)	กรอบการกำกับดูแล โครงสร้าง บทบาท หน้าที่ กระบวนการ และมาตรการควบคุมที่องค์กรกำหนดขึ้นเพื่อกำกับดูแลการพัฒนา การจัดหา การใช้งาน และการบริหารจัดการระบบ AI ให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ ระดับความเสี่ยง กฎหมาย ข้อกำหนด และหลักธรรมาภิบาลขององค์กร
8. ระบบบริหารจัดการปัญญาประดิษฐ์ (AI Management System: AIMS)	ระบบหรือกรอบการบริหารจัดการที่องค์กรกำหนดขึ้นเพื่อสนับสนุนการกำกับดูแล การบริหารจัดการความเสี่ยง การควบคุม การติดตาม และการปรับปรุงการใช้งานระบบ AI อย่างเป็นระบบและต่อเนื่อง
9. ความเสี่ยงด้านระบบ AI (AI Risk)	ความเสี่ยงที่เกิดจากการพัฒนา การจัดหา การใช้งาน หรือการกำกับดูแลระบบ AI ซึ่งอาจส่งผลกระทบต่อการดำเนินงาน ความถูกต้อง ความเป็นธรรม ความโปร่งใส ความมั่นคงปลอดภัย การปฏิบัติตามข้อกำหนด ชื่อเสียง หรือผู้มีส่วนได้เสียขององค์กร
10. ระบบ AI ที่มีความเสี่ยงสูง (High-Risk AI System)	ระบบ AI ที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อผู้มีส่วนได้เสีย สิทธิของบุคคล ความปลอดภัย การให้บริการ การดำเนินงาน หรือชื่อเสียงขององค์กร และจำเป็นต้องได้รับการกำกับดูแลหรือมาตรการควบคุมเพิ่มเติมตามที่องค์กรกำหนด
11. การกำกับดูแลโดยมนุษย์ (Human Oversight)	กระบวนการหรือกลไกที่ทำให้มนุษย์ยังคงมีบทบาทในการกำกับ ควบคุม ตรวจสอบ ทบทวน หรือแทรกแซงการทำงาน ผลลัพธ์ หรือการตัดสินใจของระบบ AI ตามความเหมาะสม เพื่อให้การใช้งานระบบ AI เป็นไปอย่างปลอดภัย มีความรับผิดชอบ และสอดคล้องกับข้อกำหนดที่เกี่ยวข้อง
12. ความสามารถในการอธิบายผลลัพธ์ (Explainability)	ความสามารถในการอธิบายหรือทำความเข้าใจหลักการทำงาน เหตุผล หรือปัจจัยที่ส่งผลต่อผลลัพธ์หรือการตัดสินใจของระบบ AI ได้ในระดับที่เหมาะสมกับลักษณะการใช้งาน ระดับความเสี่ยง และผู้มีส่วนได้เสียที่เกี่ยวข้อง
13. ความโปร่งใสของระบบ AI (AI Transparency)	การเปิดเผยหรือสื่อสารข้อมูลที่เกี่ยวข้องกับระบบ AI อย่างเหมาะสม เพื่อให้ผู้ใช้งานหรือผู้มีส่วนได้เสียสามารถเข้าใจวัตถุประสงค์ ขอบเขต ข้อจำกัด และผลกระทบที่เกี่ยวข้องกับการใช้งานระบบ AI ได้ตามความเหมาะสม

คำศัพท์	ความหมาย
14. มาตรการควบคุมพื้นฐาน (Baseline Controls)	มาตรการควบคุมขั้นต่ำที่บริษัทกำหนดสำหรับการพัฒนา การจัดหา การนำไปใช้ และการใช้งานระบบ AI เพื่อสนับสนุนการใช้งานอย่างเหมาะสม ความมั่นคงปลอดภัย การคุ้มครองข้อมูล ความรับผิดชอบของผู้ใช้งาน และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง
15. ข้อมูลอ่อนไหว (Sensitive Data)	ข้อมูลส่วนบุคคล ข้อมูลสุขภาพ ข้อมูลทางการเงิน หรือข้อมูลอื่นที่มีความอ่อนไหวตามกฎหมาย ข้อกำหนด หรือหลักเกณฑ์ขององค์กร ซึ่งจำเป็นต้องได้รับการคุ้มครองและควบคุมการเข้าถึงในระดับที่เหมาะสม
16. ทะเบียนระบบ AI (AI Inventory)	รายการหรือฐานข้อมูลที่องค์กรจัดทำขึ้นเพื่อใช้ในการระบุ บันทึก และติดตามข้อมูลที่เกี่ยวข้องกับระบบ AI ภายใต้การกำกับดูแลขององค์กร รวมถึงข้อมูลด้านวัตถุประสงค์ ผู้รับผิดชอบ ระดับความเสี่ยง สถานะการใช้งาน และข้อมูลที่เกี่ยวข้องอื่น
17. เจ้าของระบบ AI (AI System Owner)	บุคคลหรือหน่วยงานที่ได้รับมอบหมายให้รับผิดชอบในการกำกับดูแล การบริหารจัดการความเสี่ยง การควบคุม และการใช้งานระบบ AI ให้เป็นไปตามนโยบาย ข้อกำหนด และวัตถุประสงค์ที่องค์กรกำหนด
18. การประเมินผลกระทบของระบบ AI (AI System Impact Assessment: AIIA)	กระบวนการประเมินผลกระทบ ความเสี่ยง และผลที่อาจเกิดขึ้นจากการพัฒนา การจัดหา หรือการใช้งานระบบ AI ต่อผู้มีส่วนได้เสีย การดำเนินงาน สิทธิของบุคคล ความปลอดภัย จริยธรรม และข้อกำหนดที่เกี่ยวข้อง เพื่อสนับสนุนการกำหนดมาตรการควบคุมและการกำกับดูแลที่เหมาะสม

4. **บริบทองค์กรและผู้มีส่วนได้เสีย** (Context of Organization and Stakeholders)

บริษัทกำหนดกรอบการพิจารณาบริบทองค์กรและผู้มีส่วนได้เสียที่เกี่ยวข้องกับการพัฒนา การจัดหา การนำมาใช้ และการใช้งานระบบ AI เพื่อใช้เป็นกรอบในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านระบบ AI อย่างสอดคล้องทั่วทั้งองค์กร โดยองค์กรต้องนำกรอบดังกล่าวไปประยุกต์ใช้ให้สอดคล้องกับบริบททางธุรกิจ ลักษณะการดำเนินงาน และความเสี่ยงของตน

4.1 **บริบทองค์กร** (Organizational Context)

องค์กรต้องพิจารณาและทบทวนปัจจัยภายในและภายนอกที่อาจมีผลต่อการบรรลุวัตถุประสงค์ ประสิทธิผลของการกำกับดูแลและการใช้งานระบบ AI รวมถึงระดับความเสี่ยงที่เกี่ยวข้อง อย่างเป็นระบบ โดยอย่างน้อยต้องครอบคลุมประเด็นดังต่อไปนี้

ปัจจัยภายใน (Internal Factors)

- กลยุทธ์ วิสัยทัศน์ พันธกิจ วัตถุประสงค์ และเป้าหมายทางธุรกิจขององค์กร
- โครงสร้างองค์กร รูปแบบการกำกับดูแล สายการรายงาน และกระบวนการตัดสินใจขององค์กร
- ลักษณะการดำเนินงาน กระบวนการให้บริการ และความสำคัญเชิงธุรกิจของกิจกรรมหรือระบบงานที่เกี่ยวข้อง
- ความพร้อมด้านเทคโนโลยี ข้อมูล ระบบสารสนเทศ โครงสร้างพื้นฐาน และทรัพยากรบุคคลสำหรับการดำเนินงานด้านระบบ AI
- ระดับความเสี่ยงที่องค์กรยอมรับได้ และความสามารถในการบริหารจัดการความเสี่ยงขององค์กร
- วัฒนธรรมองค์กร ค่านิยม หลักจริยธรรม และความพร้อมต่อการเปลี่ยนแปลงด้านเทคโนโลยีและดิจิทัล
- ความสามารถในการกำกับดูแล ควบคุม ติดตาม และบริหารจัดการระบบ AI ตลอดวงจรชีวิตของระบบ

ปัจจัยภายนอก (External Factors)

- กฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดของหน่วยงานกำกับดูแลด้านการดำเนินงาน การคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยไซเบอร์ และการใช้งานระบบ AI
- แนวโน้ม เทคโนโลยี และการเปลี่ยนแปลงด้านระบบ AI รวมถึงความเสี่ยง ภัยคุกคาม และการเปลี่ยนแปลงของตลาดหรืออุตสาหกรรมที่อาจส่งผลต่อองค์กร
- ความคาดหวังของลูกค้า ผู้ป่วย ผู้ใช้บริการ ผู้มีส่วนได้เสีย และสาธารณะต่อการใช้งานระบบ AI อย่างมีความรับผิดชอบ โปร่งใส และปลอดภัย
- มาตรฐานสากล แนวปฏิบัติ หลักธรรมาภิบาล และหลักจริยธรรมด้าน
- สภาพแวดล้อมทางธุรกิจ ภาวะการแข่งขัน ความร่วมมือทางธุรกิจ และพันธมิตรเชิงกลยุทธ์ด้านระบบ AI
- ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามต่อระบบ AI และข้อมูลที่เกี่ยวข้อง

4.2 **ผู้มีส่วนได้เสีย** (Interested Parties)

องค์กรต้องระบุผู้มีส่วนได้เสียที่เกี่ยวข้องกับการใช้งานระบบ AI รวมถึงทำความเข้าใจความต้องการ ความคาดหวัง สิทธิ ผลกระทบ และความเสี่ยงที่เกี่ยวข้องของแต่ละกลุ่ม เพื่อใช้เป็นข้อมูลประกอบการกำกับดูแลและตัดสินใจอย่างเหมาะสม

4.3 **การกำหนดขอบเขตของระบบการบริหารจัดการปัญญาประดิษฐ์** (Scope of AI Management System: AIMS)

บริษัทกำหนดกรอบและข้อกำหนดขั้นต่ำสำหรับขอบเขตของระบบการบริหารจัดการปัญญาประดิษฐ์ (AI Management System: AIMS) เพื่อให้องค์กรนำไปประยุกต์ใช้ในการกำหนดและจัดทำขอบเขตการดำเนินงานของ AIMS ให้สอดคล้องกับลักษณะธุรกิจ ความเสี่ยง และรูปแบบการใช้งานระบบ AI ของตน ทั้งนี้ ขอบเขตของ AIMS ต้องได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง และต้องได้รับการทบทวนเป็นระยะ

4.4 **การทบทวนบริบทและผู้มีส่วนได้เสีย**

องค์กรต้องจัดให้มีการทบทวนบริบทขององค์กร ผู้มีส่วนได้เสีย และขอบเขตของระบบการบริหารจัดการปัญญาประดิษฐ์ (AIMS) เป็นระยะ หรือเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ ผลการทบทวนต้องได้รับการบันทึกรายงานต่อผู้มีอำนาจที่เกี่ยวข้อง และนำไปใช้ในการปรับปรุงวัตถุประสงค์ การบริหารจัดการความเสี่ยง มาตรการควบคุม และแนวทางการกำกับดูแลระบบ AI อย่างต่อเนื่อง เพื่อให้สอดคล้องกับบริบททางธุรกิจ ความเสี่ยง และข้อกำหนดที่เกี่ยวข้องที่เปลี่ยนแปลงไป

5. **การจัดประเภทระบบปัญญาประดิษฐ์ตามระดับความเสี่ยง** (Risk-Based AI System Classification)

บริษัทกำหนดแนวทางการจัดประเภทระบบ AI ตามระดับความเสี่ยงและวัตถุประสงค์การใช้งาน เพื่อใช้เป็นกลไกสำคัญในการกำกับดูแล การบริหารจัดการความเสี่ยง และการกำหนดมาตรการควบคุมที่เหมาะสมตามหลักการกำกับดูแลตามระดับความเสี่ยง (Risk-Based Approach) โดยองค์กรต้องนำแนวทางดังกล่าวไปประยุกต์ใช้ให้สอดคล้องกับบริบทการดำเนินงาน ลักษณะการใช้งาน และความเสี่ยงของระบบ AI ภายใต้ขอบเขตและข้อกำหนดที่บริษัทกำหนด

ทั้งนี้ การจัดระดับความเสี่ยงของระบบ AI ต้องพิจารณาปัจจัยที่เกี่ยวข้องอย่างเหมาะสม เช่น วัตถุประสงค์การใช้งาน ระดับความเป็นอิสระของระบบ ประเภทและความอ่อนไหวของข้อมูล ผลกระทบต่อสิทธิ เสรีภาพ ความปลอดภัย หรือผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย ความสำคัญของกระบวนการทางธุรกิจ และความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานระบบ AI

บริษัทกำหนดระดับความเสี่ยงของระบบ AI ออกเป็น 4 ระดับตามความรุนแรงของความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ดังนี้

1) **ระดับความเสี่ยงที่ยอมรับไม่ได้** (Unacceptable Risk)

ระบบ AI ที่ก่อให้เกิดหรืออาจก่อให้เกิดผลกระทบร้ายแรงต่อสิทธิ เสรีภาพ ความปลอดภัย ความเป็นส่วนตัว หรือศักดิ์ศรีความเป็นมนุษย์ รวมถึงระบบ AI ที่ขัดต่อกฎหมาย หลักจริยธรรม หรือหลักธรรมาภิบาลขององค์กร และไม่สามารถบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ องค์กรต้องไม่พัฒนา จัดหา นำไปใช้ หรืออนุญาตให้ใช้งานระบบ AI ดังกล่าว

ตัวอย่างระบบ AI ในระดับความเสี่ยงที่ยอมรับไม่ได้

- ระบบให้คะแนนพฤติกรรมทางสังคม (Social Scoring) ที่ประเมินหรือจัดลำดับบุคคลจากพฤติกรรมทางสังคมโดยไม่เป็นธรรม
- ระบบ AI ที่ใช้ชักจูง บิดเบือน หรือมีอิทธิพลต่อพฤติกรรมของบุคคลอย่างมีนัยสำคัญโดยไม่เหมาะสม
- การใช้งานระบบ AI ที่เอาเปรียบกลุ่มบุคคลที่มีความเปราะบาง หรือก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อสิทธิขั้นพื้นฐานของบุคคล
- การใช้ระบบระบุตัวตนด้วยข้อมูลชีวมิติ (Biometric Identification) ที่ขัดต่อกฎหมาย หลักจริยธรรม หรือข้อกำหนดที่เกี่ยวข้อง
- ระบบ AI ที่ละเมิดสิทธิ ความเป็นส่วนตัว หรือศักดิ์ศรีความเป็นมนุษย์อย่างร้ายแรง
- ระบบ AI ที่มีลักษณะเลือกปฏิบัติ สร้างอคติ หรือก่อให้เกิดผลกระทบที่ไม่เป็นธรรมต่อบุคคลหรือกลุ่มบุคคลอย่างมีนัยสำคัญ

2) **ระดับความเสี่ยงสูง** (High Risk)

ระบบ AI ที่อาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อสิทธิ เสรีภาพ ความปลอดภัย สุขภาพ การเข้าถึงบริการสำคัญ หรือการตัดสินใจที่มีสาระสำคัญต่อผู้ใช้งาน ผู้มีส่วนได้ส่วนเสีย หรือองค์กร รวมถึงระบบ AI ที่มีความเป็นอิสระสูง หรือมีผลกระทบต่อกระบวนการทางธุรกิจที่มีความสำคัญ องค์กรต้องกำหนดมาตรการควบคุม การประเมินความเสี่ยง การประเมินผลกระทบ การอนุมัติ และการกำกับดูแลที่เข้มงวด รวมถึงการกำกับดูแลโดยมนุษย์ (Human Oversight) และการติดตามประเมินผลอย่างต่อเนื่องให้เหมาะสมกับระดับความเสี่ยงของระบบ

ตัวอย่างระบบ AI ในระดับความเสี่ยงสูง

- ระบบ AI ที่ใช้ในการสนับสนุนการวินิจฉัย การตัดสินใจทางการแพทย์ หรือมีผลต่อความปลอดภัยของผู้ป่วย
- ระบบ AI สำหรับการสรรหา คัดเลือก ประเมินผล หรือพิจารณาความเหมาะสมของบุคลากร
- ระบบ AI ด้านเครดิต การเงิน การประเมินความน่าเชื่อถือ หรือการพิจารณาสินเชื่อ (Credit Scoring)
- ระบบ AI ที่ใช้ในการตัดสินใจหรือสนับสนุนการตัดสินใจที่มีผลต่อสิทธิ ผลประโยชน์ หรือความปลอดภัยของบุคคล
- ระบบ AI ที่มีผลกระทบต่อการให้บริการสำคัญ โครงสร้างพื้นฐานสำคัญ หรือกระบวนการทางธุรกิจที่มีความสำคัญขององค์กร
- ระบบ AI ที่ใช้ข้อมูลอ่อนไหว หรือข้อมูลส่วนบุคคลในระดับที่อาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อผู้มีส่วนได้ส่วนเสีย

3) **ระดับความเสี่ยงจำกัด** (Limited Risk)

ระบบ AI ที่อาจมีผลกระทบต่อการรับรู้ ความเข้าใจ หรือประสบการณ์ของผู้ใช้งาน แต่ไม่ก่อให้เกิดผลกระทบรุนแรง องค์กรต้องกำหนดมาตรการด้านความโปร่งใส การเปิดเผยข้อมูล และมาตรการควบคุมที่เหมาะสม สอดคล้องกับระดับความเสี่ยง ลักษณะการใช้งาน และผลกระทบของระบบ AI

ตัวอย่างระบบ AI ในระดับความเสี่ยงจำกัด

- ระบบ Chatbot หรือ Virtual Assistant ที่มีการโต้ตอบกับผู้ใช้งาน
- ระบบ Generative AI สำหรับสร้างข้อความ ภาพ เสียง หรือสื่อดิจิทัล
- ระบบแนะนำข้อมูลหรือเนื้อหาที่ไม่ส่งผลต่อการตัดสินใจที่มีนัยสำคัญ
- ระบบ AI สำหรับสนับสนุนการให้ข้อมูลหรือการให้บริการทั่วไปแก่ผู้ใช้งาน
- ระบบ AI ที่มีการสร้างหรือปรับแต่งเนื้อหาโดยอัตโนมัติ แต่ยังอยู่ภายใต้การกำกับดูแลโดยมนุษย์ตามความเหมาะสม

4) **ระดับความเสี่ยงต่ำหรือแทบไม่มี** (Minimal Risk)

ระบบ AI ที่มีความเสี่ยงและผลกระทบในระดับต่ำ หรือแทบไม่มีผลกระทบต่อสิทธิ เสรีภาพ ความปลอดภัย หรือการตัดสินใจที่มีนัยสำคัญของผู้ใช้งานหรือผู้มีส่วนได้ส่วนเสีย โดยทั่วไปเป็นระบบ AI ที่ใช้เพื่อสนับสนุนการดำเนินงานทั่วไป เพิ่มประสิทธิภาพการทำงาน หรืออำนวยความสะดวกในการใช้งาน โดยยังคงอยู่ภายใต้มาตรการควบคุมพื้นฐาน (Baseline Controls) ตามที่บริษัทกำหนด

ตัวอย่างระบบ AI ในระดับความเสี่ยงต่ำ

- ระบบแนะนำสินค้า (Recommendation Systems) หรือการแนะนำเนื้อหาทั่วไป
- ระบบกรองอีเมลขยะ (Spam Filtering) หรือระบบจัดหมวดหมู่ข้อมูลทั่วไป
- ระบบ AI เพื่อสนับสนุนหรือเพิ่มประสิทธิภาพการทำงานภายในองค์กรที่ไม่มีผลต่อการตัดสินใจที่มีนัยสำคัญ
- ระบบ AI สำหรับการช่วยจัดรูปแบบเอกสาร สรุปข้อมูล หรือสนับสนุนงานทั่วไปภายในองค์กร
- ระบบ AI ที่ใช้เพื่ออำนวยความสะดวกในการให้บริการหรือการใช้งานทั่วไป โดยไม่มีผลกระทบโดยตรงต่อสิทธิหรือผลประโยชน์ของผู้ใช้งานหรือผู้มีส่วนได้ส่วนเสีย

ระบบที่เข้าข่ายเป็นระบบ AI ตามหลักเกณฑ์ที่บริษัทกำหนด ต้องได้รับการจำแนกระดับความเสี่ยงตามกรอบการกำกับดูแลขององค์กรก่อนการพัฒนา การจัดหา การนำมาใช้ หรือการเปลี่ยนแปลงสาระสำคัญของระบบ และต้องได้รับการทบทวนตามความเหมาะสมเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระดับความเสี่ยง ลักษณะการใช้งาน หรือผลกระทบของระบบ

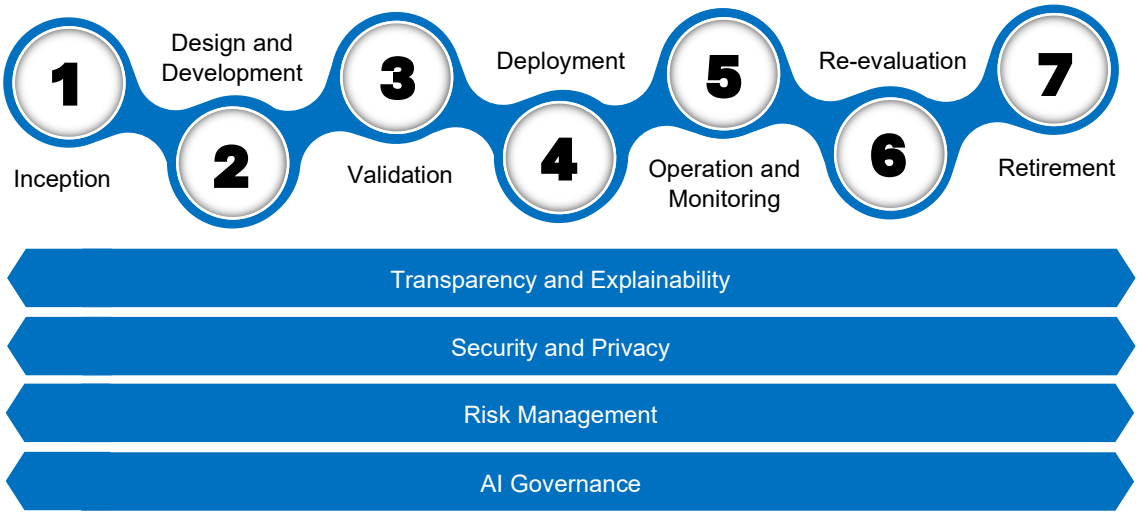
ทั้งนี้ องค์กรต้องไม่พัฒนา จัดหา หรือใช้งานระบบ AI ที่ขัดต่อกฎหมาย สิทธิมนุษยชน หรือหลักจริยธรรมพื้นฐาน รวมถึงระบบ AI ที่มีระดับความเสี่ยงที่ไม่อาจยอมรับได้ตามหลักเกณฑ์ที่บริษัทกำหนด

6. กรอบการบริหารจัดการวงจรชีวิตระบบปัญญาประดิษฐ์ (AI System Lifecycle Management Framework)

บริษัทกำหนดกรอบการบริหารจัดการวงจรชีวิตของระบบ AI เพื่อใช้เป็นแนวทางในการกำกับดูแล การพัฒนา การจัดหา การนำไปใช้ การดำเนินงาน และการยุติการใช้งานระบบ AI อย่างเป็นระบบและสอดคล้องทั่วทั้งองค์กร โดยองค์กรต้องนำกรอบดังกล่าวไปประยุกต์ใช้ให้เหมาะสมกับลักษณะธุรกิจ รูปแบบการใช้งาน และระดับความเสี่ยงของระบบ AI ภายใต้แนวทางการบริหารจัดการตามระดับความเสี่ยง

วงจรชีวิตของระบบ AI ครอบคลุมระยะสำคัญตั้งแต่การริเริ่มและกำหนดวัตถุประสงค์ การออกแบบและพัฒนา การตรวจสอบและยืนยันความเหมาะสม การนำขึ้นใช้งานจริง การดำเนินงานและการเฝ้าระวัง การทบทวนและประเมินความเหมาะสมของระบบ และการยุติการใช้งาน โดยในแต่ละระยะ องค์กรต้องคำนึงถึงหลักธรรมาภิบาล ความโปร่งใส ความรับผิดชอบ ความมั่นคงปลอดภัย ความเป็นส่วนตัว และการกำกับดูแลที่เหมาะสมตามระดับความเสี่ยงของระบบ

ทั้งนี้ องค์กรต้องกำหนดให้มีการบริหารจัดการข้อมูล เอกสาร บันทึก และหลักฐานที่เกี่ยวข้องกับระบบ AI ตลอดวงจรชีวิตของระบบ เพื่อสนับสนุนการกำกับดูแล การบริหารจัดการความเสี่ยง การตรวจสอบ และการปฏิบัติตามกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้องอย่างเหมาะสม



ภาพที่ 1 กรอบการบริหารจัดการวงจรชีวิตระบบ AI (AI System Lifecycle Management Framework)

- **การริเริ่มและกำหนดกรอบของระบบ** (AI System Inception)
  เป็นขั้นตอนในการประเมินความเหมาะสม ความจำเป็น และความสอดคล้องเชิงกลยุทธ์ของการนำระบบ AI มาใช้ในองค์กร โดยต้องกำหนดวัตถุประสงค์ ขอบเขต และกรณีการใช้งานของระบบ AI อย่างชัดเจน รวมถึงพิจารณาประโยชน์ ความเสี่ยง ผลกระทบต่อผู้มีส่วนได้เสีย และข้อกำหนดที่เกี่ยวข้อง เพื่อสนับสนุนการตัดสินใจในการพัฒนา การจัดหา หรือการใช้งานระบบ AI อย่างเหมาะสม

- **การออกแบบและพัฒนาระบบ** (AI System Design and Development)
  เป็นขั้นตอนในการกำหนดแนวทาง โครงสร้าง และองค์ประกอบของระบบ AI เพื่อให้สามารถตอบสนองต่อวัตถุประสงค์การใช้งานและข้อกำหนดที่เกี่ยวข้อง โดยต้องคำนึงถึงคุณภาพข้อมูล ความมั่นคงปลอดภัย ความเป็นส่วนตัว ความน่าเชื่อถือ ความสามารถในการอธิบายผลลัพธ์ และการกำกับดูแลโดยมนุษย์ เพื่อให้ระบบ AI อยู่ภายใต้การควบคุมและการบริหารจัดการความเสี่ยงที่เหมาะสม

- **การตรวจสอบและยืนยันความเหมาะสม** (AI System Verification and Validation)
  เป็นขั้นตอนในการประเมินความถูกต้อง ความน่าเชื่อถือ และความเหมาะสมของระบบ AI ก่อนการนำไปใช้งานจริง โดยองค์กรต้องดำเนินการทดสอบ ทวนสอบ และประเมินผลในมิติที่เกี่ยวข้อง เพื่อให้มั่นใจว่าระบบ AI สอดคล้องกับวัตถุประสงค์ ข้อกำหนด และระดับความเสี่ยงที่องค์กรยอมรับได้

- **การนำระบบขึ้นใช้งานจริง** (AI System Deployment)
  เป็นขั้นตอนในการนำระบบ AI เข้าสู่สภาพแวดล้อมการใช้งานจริงภายใต้เงื่อนไขและบริบทที่กำหนด โดยองค์กรต้องกำหนดเงื่อนไข ข้อจำกัด และแนวทางการใช้งานที่เหมาะสม รวมถึงเตรียมความพร้อมของผู้ใช้งานและผู้ที่เกี่ยวข้อง เพื่อให้การใช้งานระบบ AI เป็นไปอย่างโปร่งใสและอยู่ภายใต้การกำกับดูแลที่กำหนด

- **การดำเนินงานและการเฝ้าระวัง** (AI System Operation and Monitoring)

เป็นขั้นตอนในการติดตาม ประเมินผล และเฝ้าระวังการทำงานของระบบ AI ภายหลังการนำขึ้นใช้งานจริง โดยองค์กรต้องติดตามประสิทธิภาพ ความน่าเชื่อถือ ความเสี่ยง และเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานหรือผู้มีส่วนได้เสีย เพื่อสนับสนุนการบริหารจัดการความเสี่ยงและการตอบสนองต่อเหตุการณ์อย่างเหมาะสม

- **การทบทวนและประเมินความเหมาะสมของระบบ** (AI Re-evaluation)
  เป็นขั้นตอนในการประเมินความเหมาะสม ประสิทธิผล และระดับความเสี่ยงของระบบ AI ภายหลังการใช้งาน โดยองค์กรต้องพิจารณาการเปลี่ยนแปลงของข้อมูล เทคโนโลยี ความเสี่ยง กฎหมาย และบริบทการดำเนินงาน เพื่อสนับสนุนการตัดสินใจในการปรับปรุง ทบทวน หรือกำหนดแนวทางการใช้งานของระบบ AI อย่างเหมาะสม

- **การยุติการใช้งานระบบ** (AI System Retirement)
  เป็นขั้นตอนในการยุติหรือปลดระวางระบบ AI อย่างเป็นระบบ โดยองค์กรต้องคำนึงถึงผลกระทบต่อการดำเนินงาน ผู้มีส่วนได้เสีย ความต่อเนื่องของบริการ ข้อมูล แบบจำลอง และข้อกำหนดด้านการเก็บรักษาข้อมูล รวมถึงต้องดำเนินการภายใต้แนวทางที่สามารถควบคุม ตรวจสอบ และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

7. หลักการกำกับดูแลปัญญาประดิษฐ์ (AI Governance Principles)

บริษัทกำหนดหลักการกำกับดูแลระบบปัญญาประดิษฐ์ (AI Governance Principles) เพื่อใช้เป็นกรอบการกำกับดูแลระดับองค์กรสำหรับการพัฒนา การจัดหา การนำไปใช้ และการดำเนินงานของระบบ AI อย่างสอดคล้องและเหมาะสมทั่วทั้งองค์กร โดยครอบคลุมการกำกับดูแลตลอดวงจรชีวิตของระบบ AI และยึดหลักการบริหารจัดการความเสี่ยงตามระดับความเสี่ยง เพื่อให้การใช้งานระบบ AI สอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ การบริหารจัดการความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง

7.1 ความเป็นธรรมและไม่เลือกปฏิบัติ (Fairness)

องค์กรต้องกำหนดให้ระบบ AI ได้รับการออกแบบ พัฒนา ฝึก ทดสอบ และใช้งานโดยยึดหลักความเป็นธรรม และมีมาตรการที่เหมาะสมในการระบุ ป้องกัน ลดความเสี่ยง และติดตามความเสี่ยงจากอคติ (Bias) การเลือกปฏิบัติ หรือผลลัพธ์ที่ไม่เป็นธรรมต่อบุคคลหรือกลุ่มบุคคล ตามระดับความเสี่ยงของระบบ

7.2 จริยธรรมในการใช้งานปัญญาประดิษฐ์ (Ethics)

องค์กรต้องกำหนดให้การพัฒนา การจัดหา และการใช้งานระบบ AI เป็นไปตามหลักจริยธรรมทางวิชาชีพ หลักสิทธิมนุษยชน คุณค่าขององค์กร โดยคำนึงถึงความปลอดภัย ศักดิ์ศรีความเป็นมนุษย์ ผลประโยชน์ของผู้ป่วย ผู้รับบริการ ลูกค้า และผลกระทบทางสังคมอย่างเหมาะสม

7.3 ความรับผิดชอบและการตรวจสอบได้ (Accountability)

องค์กรต้องกำหนดและคงไว้ซึ่งโครงสร้างการกำกับดูแลระบบ AI ที่ชัดเจน โดยระบุบทบาท หน้าที่ อำนาจ และความรับผิดชอบของหน่วยงาน คณะกรรมการ และบุคลากรที่เกี่ยวข้อง ครอบคลุมตลอดวงจรชีวิตของระบบ AI ทั้งนี้ ต้องสามารถระบุผู้รับผิดชอบต่อการตัดสินใจ ผลลัพธ์ และผลกระทบที่เกิดจากระบบ AI ได้อย่างชัดเจน โปร่งใส และสามารถตรวจสอบย้อนหลังได้ เพื่อรองรับการกำกับดูแล การบริหารจัดการความเสี่ยง การตรวจสอบ และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง

7.4 ความโปร่งใสและความสามารถในการอธิบายผลลัพธ์ (Transparency & Explainability)

องค์กรต้องกำหนดให้การพัฒนา การจัดหา และการใช้งานระบบ AI มีความโปร่งใสในระดับที่เหมาะสม โดยสามารถอธิบายวัตถุประสงค์ ขอบเขตการใช้งาน หลักการทำงานในภาพรวม แหล่งที่มาของข้อมูล สมมติฐาน ข้อจำกัด และความเสี่ยงของระบบต่อผู้มีส่วนได้เสียที่เกี่ยวข้อง สำหรับระบบที่มีความเสี่ยงสูง ต้องมีระดับความสามารถในการอธิบายผลลัพธ์ที่เพียงพอต่อการสนับสนุนการตัดสินใจของมนุษย์ การทบทวน และการตรวจสอบภายหลัง

7.5 **การรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัว** (Security & Privacy)

องค์กรต้องกำหนด นำไปปฏิบัติ และคงไว้ซึ่งมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลสำหรับระบบ AI ตลอดวงจรชีวิตของระบบ โดยครอบคลุมการจำแนกข้อมูล การควบคุมสิทธิการเข้าถึง การเข้ารหัส การเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย และการตอบสนองต่อเหตุการณ์ ทั้งนี้ ต้องให้ความสำคัญเป็นพิเศษต่อข้อมูลสุขภาพ ข้อมูลอ่อนไหว และข้อมูลส่วนบุคคล ตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

7.6 **การควบคุมและกำกับดูแลโดยมนุษย์** (Human Oversight)

องค์กรกำหนดให้การใช้งานระบบ AI โดยเฉพาะกรณีที่มีผลกระทบสูงต่อความปลอดภัย สุขภาพ สิทธิของบุคคล หรือการตัดสินใจที่มีนัยสำคัญ ต้องอยู่ภายใต้การกำกับดูแลโดยมนุษย์อย่างเหมาะสมตลอดวงจรชีวิตของระบบ ทั้งนี้ องค์กรต้องกำหนดระดับการกำกับดูแลและการแทรกแซงโดยมนุษย์ให้เหมาะสมกับระดับความเสี่ยงและผลกระทบของระบบ AI และต้องมีมาตรการในการเฝ้าระวัง แทรกแซง ระงับ หรือยุติการทำงานของระบบได้อย่างทันท่วงทีเมื่อพบความเสี่ยง ความผิดพลาด หรือผลกระทบที่ไม่พึงประสงค์

8. โครงสร้างการกำกับดูแลระบบปัญญาประดิษฐ์ (AI Governance Structure)

องค์กรต้องจัดให้มีโครงสร้างการกำกับดูแลระบบปัญญาประดิษฐ์ (AI Governance Structure) ที่กำหนดอย่างเป็นทางการ มีความชัดเจน เป็นระบบ และสามารถตรวจสอบได้ เพื่อรองรับการกำหนดทิศทาง การติดตาม การควบคุม และการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับระบบ AI ตลอดวงจรชีวิตของระบบ โดยต้องมีการกำหนดบทบาท หน้าที่ ความรับผิดชอบ สายการรายงาน (Reporting Lines) ระดับอำนาจในการตัดสินใจ (Decision Authority) และกลไกการกำกับดูแล (Oversight Mechanisms) ที่เหมาะสม สอดคล้องกับระดับความเสี่ยง ลักษณะการใช้งาน และผลกระทบของระบบ AI เพื่อให้เกิดความรับผิดชอบที่ชัดเจน การตัดสินใจที่โปร่งใส สามารถตรวจสอบย้อนหลังได้ และการบริหารจัดการความเสี่ยงอย่างมีประสิทธิผล

การกำกับดูแลระบบ AI ต้องดำเนินการตามแนวทางการกำกับดูแลตามระดับความเสี่ยง (Risk-Based Governance) โดยกำหนดระดับการอนุมัติ การควบคุม และการกำกับดูแลให้เหมาะสมกับความสำคัญและผลกระทบของระบบ AI รวมถึงต้องมีการแบ่งแยกหน้าที่ (Segregation of Duties) อย่างเหมาะสมระหว่างบทบาทด้านการกำกับดูแล การพัฒนา การดำเนินงาน การบริหารจัดการความเสี่ยง การกำกับการปฏิบัติตามข้อกำหนด และการตรวจสอบ เพื่อป้องกันความขัดแย้งทางผลประโยชน์ ลดความเสี่ยงจากการใช้งาน AI ที่ไม่เหมาะสม และเสริมสร้างความน่าเชื่อถือ ความโปร่งใส และความเป็นอิสระของกระบวนการกำกับดูแล

ทั้งนี้ โครงสร้างการกำกับดูแลระบบ AI ต้องได้รับการทบทวนและปรับปรุงอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกลยุทธ์องค์กร เทคโนโลยี ความเสี่ยง กฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง

8.1 **บทบาทและความรับผิดชอบ** (Roles & Responsibilities)

องค์กรต้องกำหนดบทบาท หน้าที่ อำนาจ และความรับผิดชอบของหน่วยงาน คณะกรรมการ และบุคลากรที่เกี่ยวข้องกับระบบ AI อย่างชัดเจน เป็นลายลักษณ์อักษร และสอดคล้องกับโครงสร้างการกำกับดูแลขององค์กร เพื่อสนับสนุน

การกำกับดูแล การควบคุม และการกำหนดความรับผิดชอบอย่างเหมาะสมตลอดวงจรชีวิตของระบบ AI โดยบทบาทและความรับผิดชอบต้องครอบคลุมอย่างน้อยในด้านต่อไปนี้

- การกำหนดนโยบาย ทิศทาง กลยุทธ์ และกรอบการกำกับดูแลระบบ AI ในระดับองค์กร
- การออกแบบ พัฒนา ทดสอบ นำไปใช้งาน ดำเนินงาน และดูแลรักษาระบบ AI
- การบริหารจัดการความเสี่ยง การควบคุมภายใน ความมั่นคงปลอดภัย การคุ้มครองข้อมูล และการปฏิบัติตามข้อกำหนด
- การติดตาม สอบทาน การประเมินผล และการให้ความเชื่อมั่นหรือความเห็นอย่างเป็นอิสระ

องค์กรต้องกำหนดและประยุกต์ใช้โมเดลสามด่าน (Three Lines Model) ในการกำกับดูแลระบบ AI เพื่อให้เกิดการแบ่งแยกหน้าที่ การกำกับดูแล และการควบคุมที่มีประสิทธิผล โดยอย่างน้อยต้องประกอบด้วย

- แนวป้องกันที่หนึ่ง (First Line) รับผิดชอบการดำเนินงาน การพัฒนา การใช้งาน และการควบคุมความเสี่ยงในระดับปฏิบัติการ
- แนวป้องกันที่สอง (Second Line) รับผิดชอบด้านการกำกับดูแล การบริหารความเสี่ยง การกำหนดนโยบาย มาตรฐาน และการติดตามการปฏิบัติตามข้อกำหนด
- แนวป้องกันที่สาม (Third Line) รับผิดชอบการตรวจสอบและให้ความเชื่อมั่นอย่างเป็นอิสระต่อประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมที่เกี่ยวข้องกับ AI

ทั้งนี้ องค์กรต้องจัดให้มีกลไกการประสานงาน การสื่อสาร การรายงาน และการยกระดับประเด็นความเสี่ยงหรือเหตุการณ์สำคัญ (Escalation Mechanism) ระหว่างหน่วยงานและแนวป้องกันต่าง ๆ อย่างเหมาะสม เพื่อสนับสนุนการกำกับดูแลระบบ AI อย่างมีประสิทธิผลทั่วทั้งองค์กร

8.2 **คณะกรรมการและหน่วยงานกำกับดูแลระบบปัญญาประดิษฐ์** (AI Governance Bodies)

การกำกับดูแลระบบ AI ต้องดำเนินการผ่านคณะกรรมการ หน่วยงาน หรือกลไกการกำกับดูแลที่เหมาะสม สอดคล้องกับขนาดองค์กร ลักษณะการดำเนินธุรกิจ ระดับความซับซ้อนของการใช้งานระบบ AI และระดับความเสี่ยงที่เกี่ยวข้อง เพื่อให้การกำกับดูแล การกำหนดทิศทาง การติดตาม และการบริหารจัดการความเสี่ยงเป็นไปอย่างมีประสิทธิผล บทบาท ความรับผิดชอบ อำนาจหน้าที่ และสายการรายงานของคณะกรรมการ หน่วยงาน และผู้มีส่วนเกี่ยวข้องกับระบบ AI ต้องได้รับการกำหนดอย่างชัดเจน เป็นลายลักษณ์อักษร และสอดคล้องกับโครงสร้างการกำกับดูแลขององค์กร เพื่อรองรับการตัดสินใจ การติดตามกำกับ การยกระดับประเด็นความเสี่ยง และการกำกับดูแลที่เหมาะสมตามระดับความเสี่ยง โดยโครงสร้างการกำกับดูแลต้องเอื้อต่อการบูรณาการด้านกลยุทธ์ การบริหารจัดการความเสี่ยง การควบคุมภายใน ความมั่นคงปลอดภัย การกำกับการปฏิบัติตามข้อกำหนด และการดำเนินงานด้านระบบ AI ให้สอดคล้องกันทั่วทั้งองค์กร รวมถึงส่งเสริมความโปร่งใส ความรับผิดชอบ และการปรับปรุงอย่างต่อเนื่อง

1) **คณะกรรมการบริษัทหรือผู้บริหารระดับสูง** (Board of Directors / Executive Committee)

คณะกรรมการบริษัท ผู้บริหารระดับสูงหรือคณะกรรมการบริหารที่ได้รับมอบหมาย ต้องทำหน้าที่กำกับดูแลและกำหนดทิศทางเชิงกลยุทธ์ด้านปัญญาประดิษฐ์ (AI) ในฐานะผู้มีความรับผิดชอบสูงสุด (Ultimate Accountability) เพื่อให้มั่นใจว่าการพัฒนา การจัดหา การนำไปใช้ และการดำเนินงานของระบบ AI สอดคล้องกับวัตถุประสงค์ทาง

ธุรกิจ กลยุทธ์องค์กร กรอบการบริหารความเสี่ยง ค่านิยมองค์กร กฎหมาย กฎระเบียบ มาตรฐานที่เกี่ยวข้อง และหลักการใช้งาน AI อย่างมีความรับผิดชอบ โปร่งใส และน่าเชื่อถือ

- กำหนดวิสัยทัศน์ ทิศทางเชิงกลยุทธ์ และเป้าประสงค์ด้านระบบ AI ขององค์กร รวมถึงอนุมัตินโยบาย กรอบธรรมาภิบาล และหลักเกณฑ์การใช้งานระบบ AI ให้สอดคล้องกับกลยุทธ์องค์กร ระดับความเสี่ยงที่ยอมรับได้ และข้อกำหนดที่เกี่ยวข้อง
- กำกับดูแลให้มีการบริหารจัดการความเสี่ยง การควบคุมภายใน และมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสมตลอดวงจรชีวิตของระบบ AI รวมถึงการปฏิบัติตามกฎหมาย กฎระเบียบ มาตรฐานวิชาชีพ และข้อกำหนดด้านการกำกับดูแลที่เกี่ยวข้อง
- กำกับดูแลการจัดสรรทรัพยากรที่จำเป็น ทั้งด้านงบประมาณ บุคลากร ความรู้ความสามารถ เครื่องมือ และเทคโนโลยี เพื่อสนับสนุนการดำเนินงานและการกำกับดูแลระบบ AI อย่างมีประสิทธิผลและยั่งยืน
- รับทราบและทบทวนผลการดำเนินงาน ความเสี่ยง เหตุการณ์สำคัญ และประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบ AI พร้อมกำหนดแนวทางในการปรับปรุงและพัฒนาอย่างต่อเนื่อง เพื่อเสริมสร้างประสิทธิผลของการกำกับดูแลระบบ AI ทั่วทั้งองค์กร

2) **คณะกรรมการกำกับดูแลปัญญาประดิษฐ์** (Artificial Intelligence Governance Committee: AIGC)

บริษัทจัดให้มีคณะกรรมการกำกับดูแลปัญญาประดิษฐ์ (Artificial Intelligence Governance Committee: AIGC) หรือหน่วยงานกลางที่มีอำนาจหน้าที่เทียบเท่า เพื่อทำหน้าที่กำกับดูแลเชิงบริหาร (Management Oversight) ด้านปัญญาประดิษฐ์ในระดับองค์กร รวมถึงสนับสนุนการกำกับดูแลการใช้งาน AI อย่างเหมาะสม มีความรับผิดชอบ โปร่งใส และสอดคล้องกับหลักธรรมภิบาลองค์กร

- กำหนดและทบทวนทิศทาง เป้าหมาย ลำดับความสำคัญ และแผนการดำเนินงานด้าน AI ในระดับองค์กร ให้สอดคล้องกับกลยุทธ์องค์กร เป้าหมายทางธุรกิจ ระดับความเสี่ยงที่องค์กรยอมรับได้ และข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งนำเสนอผู้บริหารระดับสูงหรือคณะกรรมที่เกี่ยวข้องเพื่อพิจารณาและให้ความเห็นชอบตามสายการกำกับดูแลขององค์กร
- กำหนดและกำกับดูแลหลักเกณฑ์ แนวปฏิบัติและแนวทางการควบคุมที่เกี่ยวข้องกับ AI รวมถึงแนวทางการใช้งาน AI อย่างมีความรับผิดชอบ (Responsible Use of AI) เพื่อสนับสนุนการดำเนินงานด้าน AI ที่มีความมั่นคงปลอดภัย โปร่งใส ตรวจสอบได้ และสอดคล้องกับการกำกับดูแลขององค์กร
- พิจารณา ให้ความเห็นชอบ หรือยกระดับการตัดสินใจสำหรับโครงการ ระบบหรือกรณีการใช้งาน AI ที่มีความเสี่ยงสูง มีผลกระทบในวงกว้าง หรือมีนัยสำคัญต่อองค์กร ผู้ป่วย ผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย
- กำกับดูแลให้มีการประเมินความเสี่ยงด้าน AI (AI Risk Management) และประเมินผลกระทบของระบบ AI (AI Impact Assessment) อย่างเหมาะสมก่อนนำระบบไปใช้งาน รวมถึงให้มีมาตรการควบคุม การติดตาม และการทบทวนความเสี่ยงตามระดับความเสี่ยงของระบบ AI ตลอดวงจรชีวิตของระบบ
- รับทราบ ทบทวน และติดตามประเด็นสำคัญด้านกฎหมาย จริยธรรม ความมั่นคงปลอดภัย ความเป็นส่วนตัว การปฏิบัติตามข้อกำหนด และเหตุการณ์สำคัญที่เกี่ยวข้องกับระบบ AI รวมถึงการกำกับดูแลให้มีการดำเนินการแก้ไข ป้องกันและปรับปรุงที่เหมาะสม

- รายงานสถานะการกำกับดูแล ความเสี่ยง เหตุการณ์สำคัญ ผลการดำเนินงาน และประเด็นที่มีนัยสำคัญด้าน AI ต่อคณะกรรมการบริษัท ผู้บริหารระดับสูง หรือคณะกรรมการที่เกี่ยวข้องตามสายการกำกับดูแลขององค์กรอย่างสม่ำเสมอ

3) **คณะกรรมการระดับกลุ่มธุรกิจ** (Group Level Committee)

คณะกรรมการระดับกลุ่มธุรกิจ (Group Level Committee) หรือกลไกการกำกับดูแลที่มีอำนาจหน้าที่เทียบเท่า ต้องทำหน้าที่กำกับดูแลการพัฒนา การจัดหา การนำไปใช้ และการดำเนินงานของระบบ AI ในระดับกลุ่มธุรกิจ ให้สอดคล้องกับกลยุทธ์องค์กร เป้าหมายทางธุรกิจ นโยบายองค์กร กรอบการบริหารความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ โดยมุ่งเน้นการสร้างคุณค่าทางธุรกิจ การส่งเสริมนวัตกรรม และการบริหารจัดการความเสี่ยงอย่างเหมาะสม ภายใต้หลักธรรมภิบาล การกำกับดูแลกิจการที่ดี และแนวปฏิบัติสากลที่เกี่ยวข้อง

- นำนโยบาย ทิศทางและกรอบการกำกับดูแลด้าน AI ขององค์กรไปปฏิบัติ รวมถึงกำหนดและขับเคลื่อนการดำเนินงานในระดับกลุ่มธุรกิจให้สอดคล้องกับกลยุทธ์องค์กร ระดับความเสี่ยงที่ยอมรับได้ และข้อกำหนดที่เกี่ยวข้อง
- กำกับดูแลความเสี่ยง ผลกระทบ และประเด็นสำคัญที่เกิดจากการใช้ AI ในภาพรวมของกลุ่มธุรกิจ ครอบคลุมด้านจริยธรรม ความโปร่งใส ความมั่นคงปลอดภัย ความเป็นส่วนตัว ความน่าเชื่อถือและการปฏิบัติตามข้อกำหนด
- พิจารณา กลั่นกรอง ให้ความเห็นชอบหรือสนับสนุนการตัดสินใจสำหรับโครงการ ระบบหรือกรณีการใช้งานระบบ AI ที่มีนัยสำคัญ มีผลกระทบข้ามหน่วยธุรกิจ หรืออยู่ภายใต้ขอบเขตอำนาจที่ได้รับมอบหมาย
- รับทราบ ติดตามและกำกับดูแลสถานะการดำเนินงาน ความเสี่ยง และประเด็นสำคัญด้าน AI ของหน่วยธุรกิจภายใต้การกำกับดูแล รวมถึงสนับสนุนให้มีการดำเนินการแก้ไขและบริหารจัดการความเสี่ยงที่เหมาะสม
- ยกระดับประเด็นสำคัญ ความเสี่ยงที่มีนัยสำคัญ หรือเรื่องที่เกินขอบเขตอำนาจ ไปยังคณะกรรมการระดับองค์กร ผู้บริหารระดับสูง หรือหน่วยงานตามสายการกำกับดูแลขององค์กรอย่างเหมาะสมและทันท่วงที

4) **คณะกรรมการระดับหน่วยธุรกิจ** (Business Unit Level Committee)

คณะกรรมการระดับหน่วยธุรกิจ (Business Unit Level Committee) หรือหน่วยงานที่มีอำนาจหน้าที่เทียบเท่า ต้องทำหน้าที่กำกับดูแลการดำเนินงานด้านปัญญาประดิษฐ์ (AI) ในระดับหน่วยธุรกิจ เพื่อให้การนำระบบ AI ไปใช้เป็นไปตามวัตถุประสงค์ทางธุรกิจ ขอบเขตอำนาจที่ได้รับมอบหมาย และข้อกำหนดด้านการกำกับดูแลที่องค์กรกำหนด โดยมุ่งเน้นการควบคุมและติดตามการใช้งานระบบ AI ในระดับปฏิบัติการให้มีความเหมาะสม โปร่งใส สามารถตรวจสอบได้และสามารถบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิผล

- กำกับดูแลการใช้งาน AI ภายในหน่วยธุรกิจ รวมถึงการประเมินความเสี่ยง การประเมินผลกระทบของระบบ AI (AI Impact Assessment) และการกำหนดมาตรการควบคุมให้สอดคล้องกับระดับความเสี่ยง ลักษณะการใช้งาน และบริบทการดำเนินงานของหน่วยธุรกิจ
- กำกับดูแลความเสี่ยง เหตุการณ์ และประเด็นสำคัญที่เกี่ยวข้องกับระบบ AI ให้เป็นไปตามกระบวนการบริหารจัดการเหตุการณ์ การบริหารจัดการความเสี่ยง และกระบวนการยกระดับประเด็นที่องค์กรกำหนด
- ติดตาม และรายงานสถานะการดำเนินงาน ความเสี่ยง เหตุการณ์สำคัญ และประเด็นที่เกินขอบเขตอำนาจ ไปยังคณะกรรมการหรือหน่วยงานตามสายการกำกับดูแลอย่างเหมาะสมและทันท่วงที

5) **หน่วยงานเจ้าของระบบและการดำเนินงานด้านปัญญาประดิษฐ์** (AI System Owners and Operations)
หน่วยงานเจ้าของระบบและการดำเนินงานด้านปัญญาประดิษฐ์ (AI System Owners and Operations) ต้องรับผิดชอบการดำเนินงาน การควบคุม และการบริหารจัดการระบบ AI ในระดับปฏิบัติการ เพื่อให้การพัฒนา การจัดหา การนำไปใช้ และการดำเนินงานของระบบ AI เป็นไปตามวัตถุประสงค์ทางธุรกิจ ข้อกำหนดด้านคุณภาพ กรอบการกำกับดูแล ระดับความเสี่ยงที่กำหนด และข้อกำหนดด้านกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้องตลอดวงจรชีวิตของระบบ AI

- ดำเนินมาตรการควบคุม ดูแลคุณภาพ ความถูกต้อง ความพร้อมใช้งาน และความเหมาะสมของระบบ AI รวมถึงการจัดทำและดูแลทะเบียนระบบปัญญาดิษฐ์ (AI Inventory) ให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน ตลอดจนติดตามและประเมินผลการดำเนินงานของระบบอย่างต่อเนื่อง เพื่อให้มั่นใจว่าระบบยังคงมีความน่าเชื่อถือ สามารถใช้งานได้ตามวัตถุประสงค์ และสามารถบริหารจัดการความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสม
- ติดตามและประเมินสถานะความเสี่ยงของระบบ AI อย่างสม่ำเสมอ รวมถึงความเอนเอียงของผลลัพธ์ (Bias) ความผิดปกติของระบบ ความคาดเคลื่อนของผลลัพธ์ และประเด็นที่อาจส่งผลกระทบต่อการดำเนินงาน ความมั่นคงปลอดภัย หรือผู้มีส่วนได้ส่วนเสีย พร้อมดำเนินมาตรการตอบสนอง แก้ไข ฟื้นฟู และป้องกันการเกิดซ้ำตามกระบวนการที่องค์กรกำหนด
- รายงานสถานะการดำเนินงาน ความเสี่ยง เหตุการณ์สำคัญ และประเด็นที่ต้องยกระดับไปยังหน่วยงานหรือคณะกรรมการกำกับดูแลที่เกี่ยวข้องอย่างเหมาะสมและทันท่วงที เพื่อสนับสนุนการกำกับดูแล การติดตาม และการบริหารจัดการความเสี่ยงด้านระบบ AI ขององค์กรอย่างต่อเนื่องและมีประสิทธิผล

6) **หน่วยงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศระดับองค์กร** (Enterprise IT Governance Office)
หน่วยงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศระดับองค์กร (Enterprise IT Governance Office) ต้องทำหน้าที่เป็นกลไกกำกับดูแลในแนวป้องกันที่สอง (Second Line) เพื่อสนับสนุนการกำกับดูแล การบริหารจัดการความเสี่ยง และการกำกับการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศ ดิจิทัลและปัญญาประดิษฐ์ ในระดับองค์กร ให้สอดคล้องกับกลยุทธ์องค์กร กรอบการบริหารความเสี่ยง กฎหมาย กฎระเบียบ มาตรฐานที่เกี่ยวข้องและกรอบธรรมภิบาลขององค์กร

- กำหนด ทบทวน และกำกับดูแลนโยบาย มาตรฐาน และกรอบการกำกับดูแลด้าน AI ขององค์กร รวมถึงสนับสนุนการกำกับติดตามการปฏิบัติให้สอดคล้องกับข้อกำหนดภายในองค์กร กฎหมาย กฎระเบียบ มาตรฐานที่เกี่ยวข้อง
- สนับสนุนการบูรณาการการกำกับดูแลด้าน AI ระหว่างหน่วยงานที่เกี่ยวข้องทั่วทั้งองค์กรเพื่อส่งเสริมการดำเนินงานที่สอดคล้อง โปร่งใส สามารถตรวจสอบได้และบริหารจัดการความเสี่ยงได้อย่างมีเหมาะสม
- ติดตาม ประเมินและรายงานสถานะการกำกับดูแล การปฏิบัติตามข้อกำหนด ความเสี่ยง และประเด็นสำคัญด้าน AI ต่อผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องหรือหน่วยงานตามสายการกำกับดูแลขององค์กรอย่างสม่ำเสมอ

- ให้คำแนะนำและสนับสนุนหน่วยงานที่เกี่ยวข้องในการประยุกต์ใช้กรอบธรรมาภิบาล การบริหารความเสี่ยงและมาตรการควบคุมด้าน AI ให้สอดคล้องกับระดับความเสี่ยงและบริบทการดำเนินงานขององค์กร
- ส่งเสริมความรู้ ความตระหนัก และวัฒนธรรมการใช้งาน AI อย่างมีความรับผิดชอบ รวมถึงสนับสนุนการสื่อสาร การฝึกอบรม และการกำหนดแนวทางที่เหมาะสมสำหรับการใช้งาน AI ภายในองค์กร

7) **หน่วยงานตรวจสอบภายใน** (Internal Audit)

หน่วยงานตรวจสอบภายใน (Internal Audit) ต้องทำหน้าที่เป็นกลไกการให้ความเชื่อมั่นอย่างเป็นอิสระ (Independent Assurance) ในแนวป้องกันที่สาม (Third Line) เพื่อประเมินความเพียงพอ ความเหมาะสมและประสิทธิผลของการกำกับดูแล การบริหารจัดการความเสี่ยง และการควบคุมภายในที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดิจิทัล และระบบปัญญาประดิษฐ์ขององค์กร รวมถึงสนับสนุนการปฏิบัติตามนโยบายองค์กร หลักธรรมาภิบาล กฎหมาย กฎระเบียบ มาตรฐานที่เกี่ยวข้อง และการปรับปรุงประสิทธิผลของการดำเนินงานอย่างต่อเนื่อง

- ให้ความเชื่อมั่นอย่างเป็นอิสระต่อความเพียงพอ ความเหมาะสม และประสิทธิผลของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในที่เกี่ยวข้องกับปัญญาประดิษฐ์ขององค์กร
- ประเมินความเหมาะสมและประสิทธิผลของกระบวนการกำกับดูแล การบริหารจัดการความเสี่ยง และมาตรการควบคุมตลอดวงจรชีวิตของระบบ AI ให้สอดคล้องกับนโยบายองค์กร มาตรฐานสากล และข้อกำหนดที่เกี่ยวข้อง
- รายงานผลการตรวจสอบ ประเด็นความเสี่ยงที่มีนัยสำคัญ ข้อสังเกตุ และข้อเสนอแนะต่อคณะกรรมการตรวจสอบ (Audit Committee) อย่างเป็นอิสระ
- ติดตามและประเมินความเพียงพอ รวมถึงประสิทธิผลของการดำเนินการแก้ไขสำหรับประเด็นที่ตรวจพบข้อบกพร่องของการควบคุม หรือประเด็นความเสี่ยงที่เกี่ยวข้องกับ AI

8.3 อำนาจการพิจารณาและอนุมัติระบบปัญญาประดิษฐ์ (AI Decision Rights and Approval Authority)

องค์กรต้องกำหนดระดับอำนาจในการพิจารณา อนุมัติ การตัดสินใจ และการกำกับดูแลระบบปัญญาประดิษฐ์ให้สอดคล้องกับระดับความเสี่ยง ผลกระทบ ความสำคัญของระบบ และบริบทการใช้งาน เพื่อให้การกำกับดูแล การควบคุม และการบริหารจัดการความเสี่ยงเป็นไปอย่างเหมาะสม โปร่งใส สามารถตรวจสอบย้อนหลังได้ และสอดคล้องกับกรอบธรรมาภิบาล ระดับความเสี่ยงที่องค์กรยอมรับได้ ตลอดจนสนับสนุนการใช้ AI เพื่อสร้างคุณค่าทางธุรกิจ ส่งเสริมนวัตกรรม และเพิ่มประสิทธิภาพในการดำเนินงาน

ระดับความเสี่ยงของระบบ AI	การพิจารณาอนุมัติและอำนาจการตัดสินใจ
1. ระบบ AI ที่มีความเสี่ยงที่ไม่อาจยอมรับได้ (Unacceptable Risk AI Systems)	- ห้ามพัฒนา จัดหา นำไปใช้ หรือใช้งาน เว้นแต่ได้รับอนุญาตตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้องโดยเฉพาะ - ต้องได้รับการยกระดับและรายงานต่อคณะกรรมการกำกับดูแลระบบระบบปัญญาประดิษฐ์หรือผู้บริหารระดับสูงทันที
2. ระบบ AI ระดับความเสี่ยงสูง (High Risk AI Systems)	- ต้องได้รับการพิจารณา อนุมัติ หรือยกระดับการตัดสินใจโดยคณะกรรมการกำกับดูแลระบบปัญญาประดิษฐ์หรือหน่วยงานที่ได้รับมอบหมายตามขอบเขตอำนาจที่กำหนด

ระดับความเสี่ยงของระบบ AI	การพิจารณาอนุมัติและอำนาจการตัดสินใจ
3. ระบบ AI ระดับความเสี่ยงจำกัด (Limited Risk AI Systems)	- ต้องได้รับการพิจารณา อนุมัติ หรือกำกับดูแลโดยคณะกรรมการระดับกลุ่มธุรกิจ หรือผู้มีอำนาจตามขอบเขตอำนาจที่ได้รับมอบหมาย โดยให้สอดคล้องกับนโยบาย หลักเกณฑ์ และมาตรการกำกับดูแลที่องค์กรกำหนด รวมทั้งต้องกำหนดหน่วยงานหรือผู้รับผิดชอบที่ชัดเจน ทั้งนี้ ต้องมีการประเมินความเสี่ยง ทบทวน และรายงานต่อคณะกรรมการกำกับดูแลระบบปัญญาประดิษฐ์ตามรอบระยะเวลาหรือแนวทางที่องค์กรกำหนด เพื่อสนับสนุนการกำกับดูแลและติดตามการใช้งาน AI ในระดับองค์กร
4. ระบบ AI ระดับความเสี่ยงต่ำหรือความเสี่ยงน้อย (Minimal Risk AI Systems)	- ต้องได้รับการอนุมัติหรือกำกับดูแลโดยคณะกรรมการระดับหน่วยธุรกิจ หรือผู้มีอำนาจตามขอบเขตอำนาจที่ได้รับมอบหมาย โดยให้สอดคล้องกับนโยบาย หลักเกณฑ์ และมาตรการกำกับดูแลที่องค์กรกำหนด รวมทั้งต้องกำหนดหน่วยงานหรือผู้รับผิดชอบที่ชัดเจน ทั้งนี้ องค์กรอาจกำหนดให้มีการบันทึกหรือรายงานข้อมูลการใช้งานระบบ AI ตามความเหมาะสม เพื่อสนับสนุนการกำกับดูแลและการติดตามการใช้งาน AI ในระดับองค์กร

กรณีมีการเปลี่ยนแปลงสาระสำคัญ เหตุการณ์ความเสี่ยง หรือปัจจัยที่อาจส่งผลกระทบต่อระดับความเสี่ยงของระบบ AI องค์กรต้องกำหนดให้มีการประเมินผลกระทบและระดับความเสี่ยงใหม่ รวมถึงพิจารณาการยกระดับอำนาจการพิจารณาอนุมัติ หรือเสนอขออนุมัติใหม่ตามกระบวนการที่กำหนด ทั้งนี้ ต้องจัดเก็บหลักฐานการพิจารณา การอนุมัติ การตัดสินใจ และการยกระดับประเด็นที่เกี่ยวข้องอย่างเหมาะสม เพื่อรองรับการตรวจสอบย้อนหลัง ความโปร่งใส และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง

9. การกำกับดูแลและความเสี่ยงของปัญญาประดิษฐ์ (AI Governance and Risk Oversight)

องค์กรต้องจัดให้มีการกำกับดูแล การบริหารจัดการความเสี่ยง และการปฏิบัติตามข้อกำหนดด้านระบบ AI อย่างเป็นระบบ เพื่อให้การพัฒนา การจัดหา และการใช้งานเป็นไปอย่างมีความรับผิดชอบ โปร่งใส ปลอดภัย สามารถตรวจสอบได้ และสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ ระดับความเสี่ยงที่ยอมรับได้ กฎหมาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้อง

9.1 การกำกับดูแลและความรับผิดชอบของผู้บริหาร (AI Governance & Accountability)

องค์กรต้องจัดให้มีการกำกับดูแลระบบ AI ในระดับคณะกรรมการหรือผู้บริหารระดับสูง เพื่อให้มั่นใจว่าการใช้งานระบบ AI สอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ขององค์กร มีความรับผิดชอบ โปร่งใส และอยู่ภายใต้การบริหารความเสี่ยงที่เหมาะสม

9.1.1 องค์กรต้องกำหนดนโยบาย ทิศทาง และหลักการในการใช้งานระบบ AI ให้สอดคล้องกับกลยุทธ์ วัตถุประสงค์ และระดับความเสี่ยงที่องค์กรยอมรับได้

9.1.2 องค์กรต้องกำหนดบทบาท หน้าที่ ความรับผิดชอบ และสายการรายงานด้านการใช้งานระบบ AI อย่างชัดเจนในทุกระดับขององค์กร เพื่อให้เกิดความรับผิดชอบต่อผลลัพธ์จากการใช้งานระบบ AI โดยความรับผิดชอบขั้น

สูงสุดต้องอยู่ภายใต้คณะกรรมการหรือผู้บริหารระดับสูง และไม่สามารถมอบหมาย (Non-delegable accountability) ให้แก่บุคคล ระบบ หรือผู้ให้บริการภายนอกได้ ทั้งนี้ ระบบ AI ไม่ถือเป็นผู้รับผิดชอบต่อผลลัพธ์ที่เกิดขึ้น และความรับผิดชอบดังกล่าวครอบคลุมถึงการใช้ข้อมูลจากทั้งแหล่งภายในและภายนอกองค์กร

9.1.3 องค์กรต้องจัดให้มีกลไกการกำกับดูแลเฉพาะทางสำหรับระบบหรือกรณีการใช้งานที่มีความเสี่ยงหรือผลกระทบสูง เช่น คณะกรรมการพิจารณาด้านจริยธรรม (Ethics Review Board) หรือกลไกอื่นที่เหมาะสม เพื่อสนับสนุนการพิจารณาและกำกับดูแลอย่างรอบด้าน

9.1.4 องค์กรต้องกำกับดูแลการใช้งานระบบ AI ตลอดวงจรชีวิต โดยต้องพิจารณาอย่างรอบด้านในด้านประโยชน์เชิงกลยุทธ์ ความเสี่ยง ผลกระทบ และข้อกำหนดที่เกี่ยวข้อง รวมถึงความเสี่ยงจากข้อมูล แบบจำลอง และองค์ความรู้ที่ยังคงอยู่ในระบบ

9.1.5 องค์กรต้องกำกับดูแลให้มีการประเมิน (Evaluate) กำหนดทิศทาง (Direct) และติดตาม (Monitor) การใช้งานระบบ AI อย่างต่อเนื่อง รวมถึงการประเมินประสิทธิผลและคุณค่าที่ได้รับ โดยคำนึงถึงลักษณะของระบบที่อาจมีการเรียนรู้หรือปรับเปลี่ยนพฤติกรรมได้

9.1.6 องค์กรต้องกำหนดให้มีการกำกับดูแลโดยมนุษย์ที่เหมาะสมกับลักษณะการใช้งาน ระดับความเสี่ยง และผลกระทบของระบบ AI โดยต้องกำหนดบทบาท อำนาจหน้าที่ และกลไกการกำกับดูแลที่ชัดเจน เพื่อรองรับการติดตาม การทบทวน การยกระดับประเด็นความเสี่ยง และการดำเนินการเมื่อพบความผิดปกติหรือความเสี่ยงที่อาจส่งผลกระทบต่อองค์กรหรือผู้มีส่วนได้เสีย ทั้งนี้ ต้องกำกับดูแลให้ระบบ AI มีความโปร่งใสและสามารถอธิบายได้ในระดับที่เหมาะสม

9.1.7 องค์กรต้องกำหนดให้มีการสื่อสารและรายงานต่อผู้มีส่วนได้เสียภายนอกในระดับที่สอดคล้องกับความเสี่ยง ลักษณะการใช้งาน และข้อกำหนดที่เกี่ยวข้อง เพื่อสะท้อนความโปร่งใสและความรับผิดชอบขององค์กร

9.2 การกำกับดูแลการตัดสินใจที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์ (AI Decision Governance)

องค์กรต้องกำหนดและคงไว้ซึ่งกรอบการกำกับดูแลการตัดสินใจที่เกี่ยวข้องกับระบบ AI เพื่อให้การตัดสินใจที่มีระบบ AI สนับสนุน ขับเคลื่อน หรือมีส่วนเกี่ยวข้อง เป็นไปอย่างเหมาะสม โปร่งใส สามารถอธิบายได้ อยู่ภายใต้การควบคุม และมีความรับผิดชอบต่อผลลัพธ์ ทั้งนี้ ต้องสอดคล้องกับระดับความเสี่ยง วัตถุประสงค์ทางธุรกิจ กฎหมาย ข้อกำหนดที่เกี่ยวข้อง และสิทธิของผู้มีส่วนได้เสีย โดยเฉพาะกรณีที่การตัดสินใจดังกล่าวอาจส่งผลกระทบต่อผู้ป่วย ผู้ใช้บริการ บุคคล หรือการดำเนินงานที่มีนัยสำคัญขององค์กร

9.2.1 องค์กรต้องกำหนดขอบเขตการใช้งานและระดับความเป็นอิสระ (Autonomy) ของระบบ AI ในการตัดสินใจอย่างชัดเจน โดยระบุกรณีที่ระบบสามารถดำเนินการได้โดยอัตโนมัติ และกรณีที่ต้องมีการอนุมัติหรือการตัดสินใจโดยมนุษย์ ทั้งนี้ การกำหนดระดับความเป็นอิสระต้องสอดคล้องกับระดับความเสี่ยง ผลกระทบ และความสำคัญของการตัดสินใจ รวมถึงต้องคำนึงถึงข้อจำกัดของระบบ AI ในการประมวลผลบริบท

9.2.2 องค์กรต้องกำหนดบทบาท หน้าที่ อำนาจ และความรับผิดชอบต่อผลลัพธ์ของการตัดสินใจจากระบบ AI อย่างชัดเจน ไม่ว่าการตัดสินใจนั้นจะเป็นแบบอัตโนมัติ แบบมีมนุษย์ร่วมตัดสินใจ (Human-in-the-Loop) หรือแบบ

มนุษย์กำกับดูแล (Human-on-the-Loop) โดยความรับผิดชอบขั้นสุดท้ายยังคงเป็นขององค์กรและผู้มีอำนาจตัดสินใจที่ได้รับมอบหมาย

9.2.3 องค์กรต้องจัดให้มีการกำกับดูแลโดยมนุษย์สำหรับการตัดสินใจที่มีความเสี่ยงสูงหรือมีผลกระทบอย่างมีนัยสำคัญ โดยบุคลากรที่เกี่ยวข้องต้องมีความรู้และความสามารถในการตีความผลลัพธ์ ประเมินความเหมาะสม และสามารถแทรกแซง ระงับ หรือยับยั้งการตัดสินใจได้ตามความจำเป็น

9.2.4 องค์กรต้องกำหนดให้การใช้ AI ในกระบวนการตัดสินใจมีความโปร่งใสตามระดับความเสี่ยง และสามารถอธิบายได้ในระดับที่เหมาะสม โดยครอบคลุมวัตถุประสงค์ แหล่งข้อมูล ปัจจัยสำคัญของผลลัพธ์ สมมติฐาน และข้อจำกัดของระบบ รวมถึงต้องมีการบันทึกการตัดสินใจ (Decision Logging) เพื่อรองรับการตรวจสอบและการอธิบายต่อผู้มีส่วนได้เสีย

9.2.5 องค์กรต้องจัดให้มีกลไกในการตรวจสอบ ทบทวน แก้ไข ยกเลิก หรือยกระดับผลการตัดสินใจของระบบ AI โดยคำนึงถึงลักษณะผลลัพธ์เชิงความน่าจะเป็น (Probabilistic Outcomes) ความไม่แน่นอนของแบบจำลอง และข้อจำกัดของระบบ

9.2.6 องค์กรต้องจัดให้มีกลไกสำหรับการขอทบทวน อุทธรณ์ หรือท้าทายผลการตัดสินใจของระบบ AI รวมถึงช่องทางสำหรับผู้มีส่วนได้เสียในการรายงานผลลัพธ์ที่ไม่เหมาะสม เพื่อให้สามารถดำเนินการตรวจสอบและตอบสนองได้อย่างทันท่วงที

9.2.7 องค์กรต้องกำกับดูแลให้การตัดสินใจที่เกี่ยวข้องกับระบบ AI อยู่ภายใต้ดุลยพินิจและความรับผิดชอบของมนุษย์ โดยต้องคำนึงถึงข้อจำกัดของระบบ AI และป้องกันการพึ่งพาระบบเกินขอบเขต ทั้งนี้ การบริหารความเสี่ยงที่เกี่ยวข้องให้เป็นไปตามกรอบการบริหารความเสี่ยงขององค์กร

9.3 ธรรมาภิบาลการใช้ข้อมูลสำหรับระบบปัญญาประดิษฐ์ (AI Privacy and Data Governance)

องค์กรต้องกำหนดและคงไว้ซึ่งกรอบธรรมาภิบาลข้อมูลสำหรับระบบ AI เพื่อให้ข้อมูลมีคุณภาพ ความเหมาะสม ความน่าเชื่อถือ และได้รับการคุ้มครองตลอดวงจรชีวิตของข้อมูล โดยสอดคล้องกับวัตถุประสงค์การใช้งาน ระดับความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง

9.3.1 องค์กรต้องกำกับดูแลให้ข้อมูลที่ใช้สำหรับระบบ AI มีความเหมาะสม เพียงพอ และสอดคล้องกับวัตถุประสงค์การใช้งาน โดยต้องพิจารณาคุณภาพข้อมูล ความน่าเชื่อถือ ข้อจำกัด สมมติฐาน และบริบทของข้อมูลอย่างเหมาะสม เพื่อสนับสนุนความโปร่งใส ความสามารถในการตรวจสอบ และการใช้งานระบบ AI อย่างมีความรับผิดชอบ

9.3.2 องค์กรต้องกำหนดหลักเกณฑ์ในการบริหารจัดการคุณภาพข้อมูล (Data Quality) และความเหมาะสมของข้อมูล (Fit for Purpose) เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน ทันสมัย และสอดคล้องกับวัตถุประสงค์ของการใช้งานระบบ AI โดยคำนึงถึงความเพียงพอของข้อมูลในด้านปริมาณ ความเป็นปัจจุบัน บริบทของข้อมูล และความเหมาะสมเชิงต้นทุนในการนำข้อมูลไปใช้งาน

9.3.3 องค์กรต้องกำกับดูแลการจัดหา การใช้ การจัดเก็บ การแบ่งปัน การเปิดเผย และการทำลายข้อมูลอย่างเหมาะสม เพื่อป้องกันการใช้ข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหล การสูญหาย หรือการใช้งานที่ไม่สอดคล้องกับวัตถุประสงค์ที่กำหนด

9.3.4 องค์กรต้องกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยของข้อมูล และการควบคุมการเข้าถึงข้อมูลให้สอดคล้องกับกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง รวมถึงข้อจำกัดด้านลิขสิทธิ์ สิทธิในทรัพย์สินทางปัญญา และพันธสัญญาทางธุรกิจ

9.3.5 องค์กรต้องกำหนดข้อจำกัดและมาตรการควบคุมที่เหมาะสมในการนำข้อมูลขององค์กร ข้อมูลลูกค้า ข้อมูลภายใน หรือข้อมูลที่มีข้อจำกัดด้านการเปิดเผย ไปใช้กับระบบ AI เพื่อวัตถุประสงค์ส่วนบุคคล หรือระบบ AI ที่องค์กรไม่ได้อนุมัติ เว้นแต่ได้รับอนุญาตตามกระบวนการ นโยบาย มาตรฐาน และข้อกำหนดที่องค์กรกำหนด

9.3.6 องค์กรต้องกำหนดให้มีการระบุ ประเมิน และบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูล เช่น ความไม่ถูกต้อง ความไม่ครบถ้วน ความลำเอียงของข้อมูล การใช้ข้อมูลไม่เหมาะสม หรือความเสี่ยงจากการใช้ข้อมูลในอดีต (Historical Data) ที่อาจส่งผลต่อความถูกต้อง ความเป็นธรรม หรือความเหมาะสมของผลลัพธ์จากระบบ AI

9.3.7 องค์กรต้องกำหนดมาตรการควบคุมด้านข้อมูลเพิ่มเติมสำหรับระบบ AI ที่มีความเสี่ยงสูง โดยคำนึงถึงความอ่อนไหวของข้อมูล ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย ความสำคัญของกระบวนการทางธุรกิจ และความเสี่ยงจากการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยไม่เหมาะสม

9.3.8 สำหรับระบบ AI หรือบริการ AI ที่ได้รับจากผู้ให้บริการภายนอก องค์กรต้องกำหนดให้มีการประเมินและพิจารณาข้อมูลที่เกี่ยวข้องกับคุณภาพข้อมูล ข้อจำกัดของข้อมูล และแนวทางการบริหารจัดการข้อมูลเท่าที่สามารถได้รับหรือเข้าถึงได้ตามสมควร รวมถึงกำหนดมาตรการควบคุมและบริหารจัดการความเสี่ยงที่เหมาะสมตามลักษณะการใช้งาน ระดับความเสี่ยง และผลกระทบที่อาจเกิดขึ้น

9.4 **การปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง** (AI Compliance)

องค์กรต้องกำกับดูแลให้การพัฒนา การจัดหา การนำมาใช้ และการใช้งานระบบ AI เป็นไปตามกฎหมาย ระเบียบข้อบังคับ ข้อกำหนดของหน่วยงานกำกับดูแล มาตรฐานที่เกี่ยวข้อง และข้อผูกพันด้านจริยธรรมที่องค์กรยอมรับ โดยการดำเนินการอย่างถูกต้อง เหมาะสม โปร่งใส สามารถตรวจสอบได้ และสอดคล้องกับระดับความเสี่ยงของระบบอย่างต่อเนื่อง

9.4.1 องค์กรต้องจัดให้มีกระบวนการระบุ ติดตาม วิเคราะห์ และทบทวนกฎหมาย ระเบียบ ข้อกำหนด มาตรฐาน และข้อผูกพันที่เกี่ยวข้องกับระบบ AI อย่างสม่ำเสมอ เพื่อให้สามารถประเมินผลกระทบและดำเนินการได้อย่างทันท่วงที

9.4.2 องค์กรต้องกำหนดให้มีการประเมินความสอดคล้องกับข้อกำหนดที่เกี่ยวข้องก่อนการนำระบบ AI ไปใช้ ระหว่างการใช้งาน และตลอดอายุการใช้งานของระบบ โดยพิจารณาตามระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบต่อผู้มีส่วนได้เสีย

9.4.3 องค์กรต้องกำหนดมาตรการในการติดตามและปรับปรุงการใช้งานระบบ AI ให้สอดคล้องกับการเปลี่ยนแปลงของกฎหมาย ข้อกำหนด หรือมาตรฐานที่เกี่ยวข้องอย่างต่อเนื่อง โดยคำนึงถึงลักษณะของระบบ AI ที่อาจมีการเรียนรู้หรือปรับเปลี่ยนได้

9.4.4 องค์กรต้องกำหนดให้ข้อมูลที่ใช้ในการพัฒนา สร้าง หรือฝึกฝนแบบจำลองของระบบ AI เป็นไปตามกฎหมาย ระเบียบ ข้อกำหนด และนโยบายที่เกี่ยวข้องอย่างเคร่งครัด รวมถึงข้อกำหนดด้านลิขสิทธิ์ ความเป็นส่วนตัว

สิทธิในทรัพย์สินทางปัญญา และข้อจำกัดในการใช้ข้อมูล โดยต้องมีการตรวจสอบความสอดคล้องของแหล่งที่มาและสิทธิในการใช้ข้อมูลอย่างเหมาะสม

9.4.5 องค์กรต้องกำกับดูแลการใช้ระบบ AI จากผู้ให้บริการภายนอกให้เป็นไปตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง รวมถึงต้องมีการประเมินความเสี่ยง การประเมินความสอดคล้อง การบริหารสัญญา และการติดตามผลการปฏิบัติงานอย่างเหมาะสมตลอดระยะเวลาการใช้บริการ

9.4.6 องค์กรต้องจัดให้มีการจัดทำ เก็บรักษา และบริหารจัดการเอกสาร หลักฐาน และบันทึกที่เกี่ยวข้องกับระบบ AI อย่างเหมาะสม เพียงพอ และปลอดภัย เพื่อรองรับการตรวจสอบความสอดคล้อง การกำกับดูแล การสอบสวนเหตุการณ์ และการตรวจสอบย้อนหลังได้อย่างมีประสิทธิผล

9.4.7 องค์กรต้องกำกับดูแลให้การใช้ระบบ AI สอดคล้องไม่เพียงแต่กฎหมายและข้อกำหนดที่บังคับใช้เท่านั้น แต่รวมถึงข้อผูกพันโดยสมัครใจ มาตรฐานที่ยอมรับโดยทั่วไป และความคาดหวังของผู้มีส่วนได้เสียที่เกี่ยวข้องในระดับที่เหมาะสม เพื่อรักษาความเชื่อมั่น ความโปร่งใส และความน่าเชื่อถือขององค์กรอย่างต่อเนื่อง

9.5 **วัฒนธรรม ค่านิยม และจริยธรรมในการใช้ปัญญาประดิษฐ์** (Culture, Values and Ethics for AI)

องค์กรต้องกำหนดและส่งเสริมให้การใช้งานระบบ AI สอดคล้องกับค่านิยม วัฒนธรรมองค์กร และหลักจริยธรรม โดยการใช้งานต้องเป็นไปอย่างมีความรับผิดชอบ โปร่งใส เป็นธรรม และคำนึงถึงผลกระทบต่อผู้มีส่วนได้เสีย

9.5.1 องค์กรต้องส่งเสริมวัฒนธรรมการใช้งานระบบ AI อย่างมีความรับผิดชอบ โดยให้ผู้บริหารและผู้นำองค์กรมีบทบาทในการกำหนดทิศทาง เป็นแบบอย่าง และสนับสนุนการดำเนินงานด้านระบบ AI อย่างสม่ำเสมอทั่วทั้งองค์กร รวมถึงส่งเสริมการปฏิบัติตามหลักจริยธรรม กฎหมาย ข้อกำหนด และแนวปฏิบัติที่เกี่ยวข้องอย่างเหมาะสม

9.5.2 องค์กรต้องกำหนดหลักการหรือแนวปฏิบัติด้าน Responsible AI ที่สอดคล้องกับค่านิยมองค์กร หลักธรรมาภิบาล และแนวปฏิบัติสากลที่เกี่ยวข้อง เพื่อใช้เป็นกรอบในการพัฒนา การจัดหา และการใช้งานระบบ AI ให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ ระดับความเสี่ยงที่ยอมรับได้ และความรับผิดชอบต่อผู้มีส่วนได้เสียขององค์กร

9.5.3 องค์กรต้องกำหนดค่านิยม หลักจริยธรรม และพฤติกรรมที่คาดหวังในการใช้ระบบ AI อย่างชัดเจน เพื่อใช้เป็นกรอบในการตัดสินใจ การใช้งาน และการกำกับดูแลให้สอดคล้องกับเจตนารมณ์ขององค์กร

9.5.4 องค์กรต้องกำหนดให้การใช้งานระบบ AI เป็นไปตามวัตถุประสงค์และบริบทที่กำหนด (Context of Use) และต้องป้องกันการใช้งานในลักษณะที่ไม่เหมาะสมหรือขัดต่อหลักจริยธรรม

9.5.5 องค์กรต้องกำหนดมาตรการเพื่อป้องกันและลดความเสี่ยงจากการใช้งานระบบ AI ที่อาจก่อให้เกิดความลำเอียง การเลือกปฏิบัติ หรือผลกระทบเชิงลบต่อบุคคลหรือกลุ่มบุคคล

9.5.6 องค์กรต้องตระหนักถึงข้อจำกัดของระบบ AI ในการตีความบริบท การใช้วิจารณญาณ และการพิจารณาด้านจริยธรรม โดยต้องกำกับดูแลให้การใช้งานระบบอยู่ภายใต้การพิจารณาของมนุษย์ในระดับที่สอดคล้องกับความเสี่ยงและผลกระทบ เพื่อป้องกันการพึ่งพาระบบเกินขอบเขต

9.5.7 องค์กรต้องส่งเสริมให้การใช้งานระบบ AI มีความโปร่งใส สามารถอธิบายได้ และมีความรับผิดชอบต่อผลลัพธ์ที่เกิดขึ้น

9.5.8 องค์กรต้องส่งเสริมให้การใช้ระบบ AI คำนึงถึงผู้มีส่วนได้เสีย และสอดคล้องกับความคาดหวังและบรรทัดฐานของสังคมในระดับที่สอดคล้องกับความเสี่ยงและผลกระทบ เพื่อสร้างความเชื่อมั่น การยอมรับ และความไว้วางใจ รวมถึงส่งเสริมการมีส่วนร่วมของผู้มีส่วนได้เสียในกรณีที่มีผลกระทบอย่างมีนัยสำคัญ

9.6 การกำกับดูแลความเสี่ยงระบบปัญญาประดิษฐ์ (AI Risk Governance)

องค์กรกำหนดให้มีกรอบการบริหารจัดการความเสี่ยงสำหรับระบบ AI ที่สอดคล้องกับแนวทางสากล และบูรณาการเข้ากับกรอบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management: ERM) เพื่อให้การบริหารความเสี่ยงจากระบบ AI เป็นไปอย่างเป็นระบบ สอดคล้องกัน และสามารถสนับสนุนการตัดสินใจเชิงกลยุทธ์ การกำกับดูแล และการบริหารจัดการความเสี่ยงขององค์กรได้อย่างเหมาะสม

9.6.1 องค์กรต้องกำหนดให้การบริหารความเสี่ยงของระบบ AI ดำเนินการตามแนวทางตามระดับความเสี่ยง และครอบคลุมตลอดวงจรชีวิตของระบบ รวมถึงการยุติการใช้งาน โดยต้องคำนึงถึงทั้งความเสี่ยงเชิงลบและความเสี่ยงจากการพลาดโอกาส (Risk of missed opportunities)

9.6.2 องค์กรต้องกำหนดกรอบกระบวนการบริหารความเสี่ยงของระบบ AI ให้ครอบคลุมการกำหนดบริบท การระบุความเสี่ยง การวิเคราะห์และประเมินความเสี่ยง การกำหนดแนวทางจัดการความเสี่ยง การติดตามและทบทวน รวมถึงการสื่อสารและรายงานความเสี่ยง

9.6.3 องค์กรต้องกำหนดให้การบริหารความเสี่ยงคำนึงถึงลักษณะเฉพาะของระบบ AI เช่น ความไม่แน่นอนของแบบจำลอง ผลลัพธ์เชิงความน่าจะเป็น อคติของข้อมูล ความสามารถในการอธิบาย ความมั่นคงปลอดภัย ความเป็นส่วนตัว และผลกระทบต่อผู้มีส่วนได้เสีย รวมถึงแหล่งที่มาของความเสี่ยง เช่น การพึ่งพาระบบเกินสมควร ความเสี่ยงจากผู้ให้บริการภายนอก และความไม่ชัดเจนของข้อกำหนดของระบบ

9.6.4 องค์กรต้องกำหนดให้การบริหารความเสี่ยงของระบบ AI เชื่อมโยงกับกระบวนการกำกับดูแลและการตัดสินใจขององค์กร โดยต้องมีการพิจารณาระดับความเสี่ยง ผลกระทบ และความสอดคล้องกับวัตถุประสงค์ขององค์กร

9.6.5 องค์กรต้องกำกับดูแลความเสี่ยงจากการให้คุณลักษณะเชิงมนุษย์แก่ระบบ AI (Anthropomorphizing) และการพึ่งพาระบบเกินสมควร โดยต้องรักษาหลักการว่าการตัดสินใจยังคงอยู่ภายใต้ความรับผิดชอบของมนุษย์

9.6.6 องค์กรต้องกำหนดให้การบริหารความเสี่ยงของระบบ AI สอดคล้องกับกรอบการบริหารความเสี่ยงขององค์กร รวมถึงระดับความเสี่ยงที่ยอมรับได้ เกณฑ์การประเมินความเสี่ยง และการจัดประเภทความเสี่ยง โดยอาจกำหนดเกณฑ์เพิ่มเติมที่เหมาะสมกับลักษณะเฉพาะของระบบ AI

9.6.7 องค์กรต้องกำหนดและนำมาตรการจัดการและควบคุมความเสี่ยงของระบบ AI ไปใช้ให้สอดคล้องกับระดับความเสี่ยงและกรอบการควบคุมขององค์กร โดยคำนึงถึงลักษณะเฉพาะของระบบ AI เช่น การกำกับดูแลโดยมนุษย์ ข้อมูล และแบบจำลอง

9.6.8 องค์กรต้องกำหนดให้มีการติดตาม สื่อสาร รายงาน และปรับปรุงการบริหารความเสี่ยงของระบบ AI อย่างต่อเนื่อง โดยสอดคล้องกับกระบวนการบริหารความเสี่ยงขององค์กร และคำนึงถึงการเปลี่ยนแปลงของข้อมูล เทคโนโลยี และบริบทการใช้งาน

9.6.9 องค์กรต้องกำหนดให้การกำกับดูแลและการบริหารความเสี่ยงของระบบ AI ครอบคลุมถึงระบบ AI หรือบริการที่ได้รับจากผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าความเสี่ยงที่เกี่ยวข้องได้รับการกำกับดูแล ติดตาม และบริหารจัดการให้สอดคล้องกับกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและข้อกำหนดขององค์กร

10. กรอบการบริหารจัดการและควบคุมระบบปัญญาประดิษฐ์ (AI Management and Control Framework)

องค์กรต้องกำหนดและคงไว้ซึ่งกรอบการบริหารจัดการ มาตรการควบคุม และกลไกการกำกับดูแลสำหรับระบบ AI อย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยง ตลอดวงจรชีวิตของระบบ เพื่อรองรับการพัฒนา การจัดหา การนำไปใช้ การดำเนินงาน การติดตาม และการปรับปรุงระบบ AI ให้เป็นไปตามวัตถุประสงค์ทางธุรกิจ ระดับความเสี่ยงที่องค์กรยอมรับได้ กฎหมาย ข้อกำหนด และหลักการใช้งานระบบ AI อย่างมีความรับผิดชอบ

ทั้งนี้ ต้องกำหนดให้มีการจัดทำ ควบคุม จัดเก็บ และคงรักษาเอกสาร บันทึก และหลักฐานที่เกี่ยวข้องกับระบบ AI อย่างเหมาะสม เพื่อสนับสนุนการกำกับดูแล การบริหารจัดการความเสี่ยง การติดตาม การตรวจสอบ การตรวจประเมิน และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง รวมถึงต้องสามารถรองรับการตรวจสอบย้อนหลัง (Traceability) ได้ตลอดวงจรชีวิตของระบบ AI

10.1 การบริหารจัดการทรัพยากรด้านปัญญาประดิษฐ์ (AI Resource Management)

องค์กรต้องกำหนดและคงไว้ซึ่งการบริหารจัดการทรัพยากรที่เกี่ยวข้องกับระบบ AI อย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยง เพื่อรองรับการกำกับดูแล การบริหารจัดการความเสี่ยง และการดำเนินงานของระบบ AI อย่างมีประสิทธิผลตลอดวงจรชีวิตของระบบ

10.1.1 บริษัทต้องกำหนดขอบเขต หลักเกณฑ์ และแนวทางในการระบุ จัดประเภท และบริหารจัดการระบบปัญญาประดิษฐ์ภายใต้ทะเบียนระบบปัญญาประดิษฐ์ (AI Inventory) เพื่อสนับสนุนการกำกับดูแล การจัดสรรทรัพยากร การบริหารจัดการความเสี่ยง และการติดตามกำกับดูแลตลอดวงจรชีวิตของระบบ AI อย่างเหมาะสม ทั้งนี้ หลักเกณฑ์ดังกล่าวต้องคำนึงถึงลักษณะการใช้งาน วัตถุประสงค์ทางธุรกิจ ผลกระทบต่อองค์กร ระดับความเสี่ยง ประเภทและระดับความอ่อนไหวของข้อมูล ทรัพยากรที่เกี่ยวข้อง การพึ่งพาบุคคลภายนอกตลอดจนปัจจัยอื่นที่เกี่ยวข้องตามความเหมาะสม

10.1.2 องค์กรต้องจัดให้มีการบริหารจัดการทรัพยากรที่เกี่ยวข้องกับระบบ AI อย่างเพียงพอ เหมาะสมและสอดคล้องกับลักษณะการใช้งาน ระดับความเสี่ยง และความสำคัญทางธุรกิจของระบบ เพื่อสนับสนุนการดำเนินงาน การกำกับดูแล และการบริหารจัดการความเสี่ยงของระบบ AI ตลอดวงจรชีวิต

10.1.3 องค์กรต้องกำหนดให้ข้อมูลที่ใช้ในระบบ AI ได้รับการบริหารจัดการอย่างเหมาะสม โดยคำนึงถึงคุณภาพ ความครบถ้วน ความถูกต้อง ความทันสมัย และความเป็นตัวแทนของข้อมูล ทั้งนี้ การใช้ข้อมูลต้องสอดคล้องกับข้อกำหนดด้านความเป็นส่วนตัว ความมั่นคงปลอดภัย และกฎหมายที่เกี่ยวข้อง

10.1.4 องค์กรต้องกำหนดให้เครื่องมือ แพลตฟอร์ม เฟรมเวิร์ก แบบจำลอง และสภาพแวดล้อมทางเทคนิคที่ใช้สำหรับระบบ AI มีความเหมาะสมกับข้อกำหนดของระบบ โดยคำนึงถึงความน่าเชื่อถือ ความมั่นคงปลอดภัย ประสิทธิภาพ ข้อจำกัด และความสามารถในการกำกับดูแลและตรวจสอบตามความเหมาะสม

10.1.5 องค์กรต้องกำหนดให้โครงสร้างพื้นฐาน ระบบประมวลผล เครือข่าย และทรัพยากรด้านการจัดเก็บข้อมูลที่ใช้สำหรับระบบ AI มีความพร้อมใช้งาน ความเพียงพอ ความยืดหยุ่น และความมั่นคงปลอดภัยที่เหมาะสมกับภาระงานและระดับความเสี่ยงของระบบตลอดวงจรชีวิต

10.1.6 องค์กรต้องกำหนดให้ทรัพยากรหรือบริการที่ได้จากบุคคลภายนอก เช่น ข้อมูล แบบจำลอง ระบบคลาวด์ เครื่องมือ หรือบริการ AI อยู่ภายใต้การประเมินความเหมาะสม ความน่าเชื่อถือ ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้อง รวมถึงต้องสอดคล้องกับกรอบการบริหารจัดการบุคคลภายนอกด้านเทคโนโลยีสารสนเทศขององค์กร

10.1.7 องค์กรต้องกำหนดให้มีการติดตาม ตรวจสอบ และทบทวนความเพียงพอ ความเหมาะสม ประสิทธิผล และความต่อเนื่องของทรัพยากรที่เกี่ยวข้องกับระบบ AI อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าทรัพยากรถูกใช้งานตามวัตถุประสงค์ที่ได้รับอนุมัติ และยังคงสามารถรองรับการดำเนินงานและการบริหารจัดการความเสี่ยงของระบบ AI ได้อย่างเหมาะสม

10.2 การบริหารจัดการความเสี่ยงจากการใช้ปัญญาประดิษฐ์ (AI Risk Management)

องค์กรต้องกำหนดและดำเนินการกระบวนการบริหารจัดการความเสี่ยงสำหรับระบบ AI อย่างเป็นระบบ โดยครอบคลุมการระบุ การประเมิน การจัดการ การติดตาม และการรายงานความเสี่ยง เพื่อให้มั่นใจว่าความเสี่ยงจากการใช้ระบบ AI อยู่ในระดับที่องค์กรยอมรับได้ และสอดคล้องกับวัตถุประสงค์ทางธุรกิจ ข้อกำหนดทางกฎหมาย และกรอบการกำกับดูแลขององค์กร

10.2.1 องค์กรต้องกำหนดบทบาท หน้าที่ อำนาจ และความรับผิดชอบในการบริหารจัดการความเสี่ยงของระบบ AI อย่างชัดเจน รวมถึงการกำหนดผู้รับผิดชอบความเสี่ยง (Risk Owner) เพื่อรองรับการติดตาม การประเมิน และการจัดการความเสี่ยงอย่างเหมาะสม

10.2.2 องค์กรต้องกำหนดให้มีการระบุความเสี่ยงของระบบ AI อย่างเป็นระบบในทุกระยะของวงจรชีวิต โดยครอบคลุมความเสี่ยงด้านข้อมูล ระบบงาน ผู้ให้บริการภายนอก ความมั่นคงปลอดภัย ความปลอดภัย ความเป็นส่วนตัว ความเป็นธรรม ความโปร่งใส ความสามารถในการอธิบายผลลัพธ์ จริยธรรม การกำกับดูแลโดยมนุษย์ การปฏิบัติตามข้อกำหนด และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย รวมถึงความเสี่ยงที่เกี่ยวข้องกับองค์ประกอบทางเทคนิคของระบบ อาทิ แบบจำลอง อัลกอริทึม หรือองค์ประกอบสำคัญของระบบ ตามข้อมูลที่องค์กรสามารถได้รับหรือเข้าถึงได้ตามสมควร

10.2.3 องค์กรต้องกำหนดให้มีการประเมินความเสี่ยงของระบบ AI โดยใช้เกณฑ์ที่องค์กรกำหนด เช่น ระดับผลกระทบและโอกาสเกิด เพื่อจัดระดับและจัดประเภทความเสี่ยงให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้

10.2.4 สำหรับระบบ AI ที่มีความเสี่ยงสูงหรืออาจส่งผลกระทบอย่างมีนัยสำคัญต่อผู้มีส่วนได้เสีย องค์กรต้องดำเนินการประเมินผลกระทบของระบบปัญญาประดิษฐ์ (AI System Impact Assessment: AIIA) โดยครอบคลุมผลกระทบต่อผู้มีส่วนได้เสีย การดำเนินงานขององค์กร สิทธิของบุคคล ความปลอดภัย จริยธรรม และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ทั้งนี้ ผลการประเมินต้องถูกนำไปใช้ประกอบการกำหนดมาตรการควบคุม การอนุมัติการใช้งาน และการกำกับดูแลตามระดับความเสี่ยง

10.2.5 องค์กรต้องกำหนดและนำมาตรการควบคุมความเสี่ยงของระบบ AI ไปใช้ให้สอดคล้องกับระดับความเสี่ยง ลักษณะการใช้งาน และผลกระทบของระบบ โดยอาจครอบคลุมการกำกับดูแลโดยมนุษย์ การควบคุมด้านข้อมูล ความมั่นคงปลอดภัย การตรวจสอบและติดตามผลลัพธ์ การบริหารจัดการผู้ให้บริการภายนอก และ

มาตรการลดความเสี่ยงอื่นที่เกี่ยวข้อง เพื่อให้สามารถควบคุมและลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

10.2.6 องค์กรต้องกำหนดให้ผลการประเมินความเสี่ยงและผลกระทบของระบบ AI ถูกนำไปใช้ประกอบการพิจารณาอนุมัติ การกำหนดมาตรการควบคุม และการกำกับดูแลตามระดับความเสี่ยงและกระบวนการที่องค์กรกำหนด

10.2.7 องค์กรต้องกำหนดให้มีการจัดทำและดูแลรายการความเสี่ยงของระบบ AI (AI Risk Register) เพื่อใช้ในการบันทึก ติดตาม และบริหารจัดการข้อมูลความเสี่ยง มาตรการควบคุม สถานะความเสี่ยง และการดำเนินการที่เกี่ยวข้องอย่างเหมาะสม

10.2.8 องค์กรต้องกำหนดให้มีการติดตาม เฝ้าระวัง และทบทวนความเสี่ยงของระบบ AI อย่างต่อเนื่อง รวมถึงการรายงานความเสี่ยง ตัวชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) เหตุการณ์สำคัญ หรือแนวโน้มความเสี่ยงต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องตามระดับความเสี่ยงและสาระสำคัญของระบบ พร้อมมีกลไกการยกระดับประเด็นเมื่อจำเป็น

10.2.9 องค์กรต้องกำหนดให้เหตุการณ์ที่เกี่ยวข้องกับความเสี่ยงของระบบ AI อยู่ภายใต้กระบวนการบริหารจัดการเหตุการณ์ขององค์กร โดยครอบคลุมการบันทึก การตรวจจับ การรายงาน การตอบสนอง การวิเคราะห์สาเหตุ การดำเนินการแก้ไขและป้องกัน รวมถึงการติดตามผลและปรับปรุงมาตรการควบคุมอย่างต่อเนื่อง เพื่อให้สามารถลดผลกระทบจากเหตุการณ์ได้อย่างเหมาะสมและทันท่วงที

10.2.10 องค์กรต้องกำหนดให้การบริหารจัดการความเสี่ยงของระบบ AI อยู่ภายใต้การติดตามหรือการตรวจสอบตามความเหมาะสม เพื่อสนับสนุนการประเมินความสอดคล้องกับนโยบาย กระบวนการ และข้อกำหนดที่เกี่ยวข้อง รวมถึงการระบุประเด็นความเสี่ยงและโอกาสในการปรับปรุง

10.2.11 องค์กรต้องกำหนดให้มีการทบทวนการบริหารจัดการความเสี่ยงของระบบ AI ตามกระบวนการกำกับดูแลขององค์กร เพื่อสนับสนุนการประเมินความเหมาะสม ประสิทธิผล และความสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ รวมถึงการปรับปรุงอย่างต่อเนื่อง

10.2.12 องค์กรต้องกำหนดให้มีการปรับปรุงการบริหารจัดการความเสี่ยงของระบบ AI อย่างต่อเนื่อง โดยอ้างอิงจากผลการติดตามและเฝ้าระวังความเสี่ยง เหตุการณ์ความเสี่ยงหรือเหตุการณ์ผิดปกติ ผลการตรวจสอบภายในและผลการทบทวนโดยผู้บริหาร เพื่อให้มั่นใจว่ากระบวนการบริหารจัดการความเสี่ยงยังคงมีความเหมาะสม มีประสิทธิผล และสามารถรองรับการเปลี่ยนแปลงของข้อมูล เทคโนโลยี สภาพแวดล้อมทางธุรกิจ และข้อกำหนดที่เกี่ยวข้องได้อย่างต่อเนื่อง

10.3 **การบริหารจัดการวงจรชีวิตระบบปัญญาประดิษฐ์** (AI System Lifecycle Management)

องค์กรต้องกำหนดและคงไว้ซึ่งกระบวนการบริหารจัดการวงจรชีวิตของระบบ AI อย่างเป็นระบบและสอดคล้องกับระดับความเสี่ยง เพื่อรองรับการกำกับดูแล การบริหารจัดการความเสี่ยง การควบคุม การติดตาม และการปรับปรุงระบบ AI ตลอดวงจรชีวิตของระบบ ให้เป็นไปตามวัตถุประสงค์ทางธุรกิจ กฎหมาย ข้อกำหนด และนโยบายที่เกี่ยวข้องขององค์กร

10.3.1 องค์กรต้องกำหนดให้ระบบที่เข้าข่ายเป็นระบบปัญญาประดิษฐ์ (AI) ตามหลักเกณฑ์ที่บริษัทกำหนด มีการระบุวัตถุประสงค์การใช้งาน ขอบเขต บริบท สมมติฐาน และข้อจำกัดของระบบอย่างชัดเจนก่อนการพัฒนา

การจัดหา หรือการนำไปใช้งาน ทั้งนี้ ระบบดังกล่าวต้องผ่านการประเมินความเสี่ยง การประเมินผลกระทบต่อผู้มีส่วนได้ส่วนเสีย และการพิจารณาอนุมัติตามระดับอำนาจที่กำหนด

10.3.2 องค์กรต้องกำหนดข้อกำหนดของระบบปัญญาประดิษฐ์ (AI System Requirements) ให้ครอบคลุมความต้องการทางธุรกิจ เงื่อนไขการใช้งาน เกณฑ์ด้านประสิทธิภาพ ความมั่นคงปลอดภัย ความสามารถในการอธิบายผลลัพธ์ และข้อกำหนดด้านกฎหมายหรือกฎระเบียบที่เกี่ยวข้อง ทั้งนี้ การใช้งานระบบ AI ต้องไม่เกินขอบเขตที่ได้รับอนุมัติ และการเปลี่ยนแปลงวัตถุประสงค์หรือบริบทการใช้งานต้องอยู่ภายใต้กระบวนการกำกับดูแลที่กำหนด

10.3.3 องค์กรต้องกำหนดให้การออกแบบ พัฒนา หรือปรับแต่งระบบ AI เป็นไปตามข้อกำหนดของระบบ โดยคำนึงถึงคุณภาพและความเหมาะสมของข้อมูล ความเสี่ยงจากอคติของข้อมูล ความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และความเหมาะสมต่อบริบทการใช้งาน เพื่อสนับสนุนการดำเนินงานของระบบ AI อย่างเหมาะสมและสอดคล้องกับข้อกำหนดขององค์กร

10.3.4 องค์กรต้องกำหนดให้มีการทดสอบ ตรวจสอบ และยืนยันความเหมาะสมของระบบ AI ก่อนการนำไปใช้งาน เพื่อให้มั่นใจว่าระบบเป็นไปตามข้อกำหนด วัตถุประสงค์ และระดับความเสี่ยงที่องค์กรยอมรับได้ รวมถึงต้องได้รับการอนุมัติตามโครงสร้างการกำกับดูแลขององค์กร หรือได้รับข้อมูลยืนยันผลการทดสอบจากผู้ให้บริการตามความเหมาะสม ทั้งนี้ เมื่อองค์กรได้รับทราบหรือได้รับแจ้งถึงการเปลี่ยนแปลงที่มีนัยสำคัญต่อข้อมูล แบบจำลอง บริบทการใช้งาน หรือองค์ประกอบสำคัญของ AI องค์กรต้องประเมินผลกระทบและพิจารณาการดำเนินการทดสอบ ตรวจสอบ หรือยืนยันความเหมาะสมของระบบเพิ่มเติมตามระดับความเสี่ยงที่เกี่ยวข้อง

10.3.5 องค์กรต้องกำหนดให้การนำระบบ AI ไปใช้งานอยู่ภายใต้ขอบเขตที่ได้รับอนุมัติ พร้อมกำหนดบทบาทและความรับผิดชอบของผู้ใช้งานอย่างชัดเจน รวมถึงต้องมีกลไกการกำกับดูแลโดยมนุษย์ในระดับที่เหมาะสม โดยเฉพาะกรณีที่ระบบมีผลต่อการตัดสินใจที่มีนัยสำคัญ ทั้งนี้ ต้องมีการเปิดเผยข้อมูลเกี่ยวกับวัตถุประสงค์ ข้อจำกัด และลักษณะการทำงานของระบบ AI ตามที่องค์กรสามารถได้รับหรือเข้าถึงได้ตามสมควร ต่อผู้มีส่วนได้เสียตามความเหมาะสม

10.3.6 องค์กรต้องกำหนดให้มีการติดตาม ตรวจสอบ และประเมินผลการทำงานของระบบ AI ตามระดับความเสี่ยงและลักษณะการใช้งานของระบบ เพื่อให้มั่นใจว่าระบบยังคงสามารถดำเนินงานได้อย่างเหมาะสม มีเสถียรภาพ และสอดคล้องกับวัตถุประสงค์การใช้งาน ทั้งนี้ ต้องมีการบันทึก วิเคราะห์ และจัดการเหตุการณ์ผิดปกติ ความล้มเหลว หรือความเบี่ยงเบนที่มีนัยสำคัญต่อวัตถุประสงค์การใช้งาน ระดับความเสี่ยง หรือผลกระทบของระบบ AI รวมถึงกำหนดมาตรการแก้ไขและป้องกัน (Corrective and Preventive Actions) ตามความเหมาะสม

10.3.7 องค์กรต้องกำหนดให้การปรับปรุงแบบจำลอง การเปลี่ยนแปลงข้อมูล การตั้งค่า หรือการเปลี่ยนแปลงสาระสำคัญอื่นของระบบ AI ที่องค์กรดำเนินการหรือสามารถควบคุมได้ อยู่ภายใต้<u>กระบวนการควบคุมการเปลี่ยนแปลงขององค์กร</u> โดยต้องมีการประเมินความเสี่ยง ผลกระทบ และการอนุมัติตามความเหมาะสมก่อนดำเนินการ ทั้งนี้ สำหรับการเปลี่ยนแปลงที่องค์กรรับทราบจากผู้ให้บริการภายนอก องค์กรต้องประเมินผลกระทบและความเสี่ยง รวมทั้งดำเนินการตามความเหมาะสมตามระดับความเสี่ยงและลักษณะการใช้งาน

10.3.8 องค์กรต้องกำหนดจุดตัดสินใจสำคัญ (Key Decision Points) ตามความเหมาะสมในแต่ละระยะของวงจรชีวิตระบบ AI พร้อมระบุบทบาท หน้าที่ อำนาจ และผู้รับผิดชอบอย่างชัดเจน โดยการตัดสินใจต้องพิจารณาจากระดับความเสี่ยง ผลกระทบ และความสอดคล้องกับข้อกำหนดของระบบ ทั้งนี้ ต้องกำหนดเจ้าของระบบปัญญาประดิษฐ์ (AI System Owner) หรือผู้รับผิดชอบที่มีอำนาจหน้าที่เทียบเท่า รวมถึงผู้รับผิดชอบในแต่ละระยะที่เกี่ยวข้องของวงจรชีวิต เพื่อให้สามารถกำกับดูแล ติดตาม และรับผิดชอบต่อการดำเนินงานของระบบ AI ได้อย่างเหมาะสมตลอดวงจรชีวิต

10.3.9 องค์กรต้องกำหนดให้ระบบ AI อยู่ภายใต้การทบทวนตามกระบวนการกำกับดูแลขององค์กร เพื่อประเมินความเหมาะสม ประสิทธิผล ความเสี่ยง และความสอดคล้องกับวัตถุประสงค์ทางธุรกิจและข้อกำหนดที่เกี่ยวข้อง

10.3.10 องค์กรต้องกำหนดให้การยุติหรือปลดระวางระบบ AI ดำเนินการอย่างเป็นระบบ โดยคำนึงถึงผลกระทบต่อการดำเนินงาน ความต่อเนื่องของบริการ การโยกย้ายหรือทำลายข้อมูล การยกเลิกสิทธิการเข้าถึง และการเก็บรักษาหลักฐานที่จำเป็น ให้สอดคล้องกับนโยบาย กฎหมาย และข้อกำหนดที่เกี่ยวข้อง

10.4 การบริหารจัดการข้อมูลและแบบจำลอง (AI Data and Model Management)

องค์กรต้องกำหนดและคงไว้ซึ่งกระบวนการบริหารจัดการข้อมูลและแบบจำลองของระบบ AI อย่างเป็นระบบและสอดคล้องกับระดับความเสี่ยง เพื่อให้ข้อมูลและแบบจำลองสามารถรองรับการกำกับดูแล การบริหารจัดการความเสี่ยง และการใช้งานระบบ AI ได้อย่างเหมาะสมตลอดวงจรชีวิตของระบบ

10.4.1 องค์กรต้องกำหนดให้มีการบริหารจัดการข้อมูลที่ใช้สำหรับการพัฒนา ฝึกสอน ทดสอบ ตรวจสอบ และใช้งานระบบ AI อย่างเหมาะสม โดยคำนึงถึงคุณภาพ ความครบถ้วน ความถูกต้อง ความทันสมัย ความเหมาะสมของแหล่งที่มา ความเป็นตัวแทนของข้อมูล และความเสี่ยงจากอคติของข้อมูล (Data Bias)

10.4.2 องค์กรต้องกำหนดให้ข้อมูลที่ใช้ในระบบ AI สามารถระบุแหล่งที่มา (Data Provenance) และติดตามการเปลี่ยนแปลงหรือการไหลของข้อมูล (Data Lineage) ได้ในระดับที่เหมาะสม เพื่อสนับสนุนการควบคุมคุณภาพข้อมูล ความน่าเชื่อถือของข้อมูล และการตรวจสอบย้อนหลังตลอดวงจรชีวิตของระบบ

10.4.3 องค์กรต้องกำหนดให้การใช้ข้อมูลในระบบ AI เป็นไปตามวัตถุประสงค์ที่ได้รับอนุมัติ และสอดคล้องกับหลักการใช้ข้อมูลเท่าที่จำเป็น (Data Minimization) รวมถึงกฎหมาย ข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูล และนโยบายขององค์กร

10.4.4 องค์กรต้องกำหนดให้แบบจำลองของระบบ AI ได้รับการบริหารจัดการอย่างเหมาะสม โดยต้องสามารถระบุวัตถุประสงค์ ขอบเขตการใช้งาน ข้อจำกัด สมมติฐาน วิธีการพัฒนา และข้อมูลสำคัญที่ใช้ในการพัฒนาแบบจำลองได้อย่างชัดเจน

10.4.5 องค์กรต้องกำหนดให้การพัฒนา การปรับปรุง การปรับแต่ง และการใช้งานแบบจำลองของระบบ AI สามารถติดตามเวอร์ชัน สถานะ ประวัติการเปลี่ยนแปลง และผู้อนุมัติได้อย่างเหมาะสม เพื่อสนับสนุนการกำกับดูแล การบริหารจัดการความเสี่ยง และการควบคุมการเปลี่ยนแปลงของแบบจำลอง

10.4.6 องค์กรต้องกำหนดให้มีการติดตาม ทดสอบ และทบทวนประสิทธิภาพของแบบจำลองอย่างเหมาะสมตามระดับความเสี่ยง โดยครอบคลุมความแม่นยำ ความเสถียร ความเป็นธรรม ความสามารถในการอธิบาย

ผลลัพธ์ และความเหมาะสมต่อบริบทการใช้งาน เพื่อให้มั่นใจว่าผลลัพธ์ของระบบ AI ยังคงมีคุณภาพและความน่าเชื่อถืออย่างต่อเนื่อง

10.4.7 องค์กรต้องกำหนดให้ข้อมูล แบบจำลอง เครื่องมือพัฒนา และองค์ประกอบที่เกี่ยวข้องกับระบบ AI ได้รับการบริหารจัดการและควบคุมการใช้งานอย่างเหมาะสม โดยให้สอดคล้องกับบทบาทหน้าที่ วัตถุประสงค์การใช้งาน และข้อกำหนดด้านการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร

10.4.8 องค์กรต้องกำหนดให้มีการติดตามและทบทวนคุณภาพข้อมูล ความเปลี่ยนแปลงของข้อมูล (Data Drift) ความเปลี่ยนแปลงของแบบจำลอง (Model Drift) และผลกระทบจากการใช้งานแบบจำลองอย่างต่อเนื่อง เพื่อสนับสนุนการบริหารจัดการความเสี่ยง และลดผลกระทบที่อาจเกิดขึ้นต่อผู้ใช้ ผู้รับบริการ ผู้ป่วย หรือองค์กร

10.5 การรักษาความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์ (AI Security)

องค์กรต้องกำหนดและคงไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับระบบ AI อย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยง โดยครอบคลุมข้อมูล แบบจำลอง โครงสร้างพื้นฐาน ระบบงาน กระบวนการ และบุคลากรที่เกี่ยวข้อง เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ การเข้าถึงหรือการใช้งานโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล การเปลี่ยนแปลงที่ไม่เหมาะสม และเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อองค์กร ผู้ใช้บริการ ผู้ป่วย หรือผู้มีส่วนได้ส่วนเสียตลอดวงจรชีวิตของระบบ AI

10.5.1 องค์กรต้องกำหนดกรอบการกำกับดูแลและแนวทางด้านความมั่นคงปลอดภัยสำหรับระบบ AI ให้สอดคล้องกับนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร หลักการบริหารจัดการความเสี่ยง กฎหมาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้อง โดยต้องพิจารณาความเสี่ยงที่เกี่ยวข้องกับข้อมูล แบบจำลอง ระบบ AI โครงสร้างพื้นฐาน และผู้ให้บริการภายนอกตลอดวงจรชีวิตของระบบ ภายใต้แนวทางการบริหารจัดการตามระดับความเสี่ยง

10.5.2 องค์กรต้องกำหนดให้ข้อมูลที่ใช้ในระบบ AI ได้รับการคุ้มครองอย่างเหมาะสม โดยคำนึงถึงความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล (Confidentiality, Integrity, Availability) รวมถึงการจำแนกประเภทข้อมูล การเข้ารหัส การสำรองข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว ให้สอดคล้องกับกฎหมาย นโยบาย และข้อกำหนดที่เกี่ยวข้อง

10.5.3 องค์กรต้องกำหนดให้แบบจำลองของระบบ AI ได้รับการคุ้มครองและบริหารจัดการด้านความมั่นคงปลอดภัยอย่างเหมาะสม โดยครอบคลุมการป้องกันการโจมตีต่อแบบจำลอง การดัดแปลงโดยไม่ได้รับอนุญาต การรั่วไหลของแบบจำลองหรือข้อมูลฝึกสอน การละเมิดทรัพย์สินทางปัญญา การรักษาความถูกต้องของแบบจำลอง และความสามารถในการระบุแหล่งที่มาของแบบจำลองตามความเหมาะสม

10.5.4 องค์กรต้องกำหนดให้การเข้าถึงข้อมูล แบบจำลอง และระบบ AI เป็นไปตามบทบาทหน้าที่และความจำเป็นในการใช้งาน (Need-to-Know / Least Privilege) พร้อมกำหนดมาตรการยืนยันตัวตน การกำหนดสิทธิ์ และการบริหารจัดการบัญชีผู้ใช้งานอย่างเหมาะสม เพื่อป้องกันการเข้าถึง การใช้งาน หรือการเปิดเผยโดยไม่ได้รับอนุญาต รวมถึงต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

10.5.5 องค์กรต้องกำหนดให้โครงสร้างพื้นฐาน แพลตฟอร์ม เครื่องมือพัฒนา และสภาพแวดล้อมที่ใช้สำหรับการพัฒนา ทดสอบ และใช้งานระบบ AI มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยครอบคลุมการ

บริหารจัดการช่องโหว่ การกำหนดค่าที่ปลอดภัย การแบ่งแยกสภาพแวดล้อม การบริหารจัดการแพตช์ การป้องกันมัลแวร์ และมาตรการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

10.5.6 องค์กรต้องกำหนดให้มีการติดตาม ตรวจสอบ และบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบ AI อย่างเหมาะสม รวมถึงกำหนดกลไกการแจ้งเตือนเมื่อพบพฤติกรรมผิดปกติ เหตุการณ์ที่มีความเสี่ยง หรือภัยคุกคามที่อาจส่งผลกระทบต่อระบบ AI เพื่อสนับสนุนการตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที

10.5.7 องค์กรต้องกำหนดให้มีการระบุ ประเมิน และบริหารจัดการช่องโหว่และภัยคุกคามด้านความมั่นคงปลอดภัยของระบบ AI อย่างสม่ำเสมอ โดยต้องมีการจัดลำดับความสำคัญตามระดับความเสี่ยง ดำเนินการแก้ไขหรือบรรเทาความเสี่ยงภายในระยะเวลาที่เหมาะสม และปรับปรุงมาตรการควบคุมอย่างต่อเนื่อง

10.5.8 องค์กรต้องกำหนดให้เหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบ AI อยู่ภายใต้กระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยต้องมีการตอบสนอง แก้ไข กู้คืน รายงาน และยกระดับเหตุการณ์ตามระดับความรุนแรง ระดับความเสี่ยง และข้อกำหนดที่เกี่ยวข้อง

10.6 การบริหารความเสี่ยงการใช้ระบบปัญญาประดิษฐ์จากผู้ให้บริการภายนอก (Third-party AI Risk Management)

องค์กรต้องกำหนดและคงไว้ซึ่งกระบวนการบริหารความเสี่ยงสำหรับการใช้ระบบ AI หรือบริการที่เกี่ยวข้องจากผู้ให้บริการภายนอก โดยพิจารณาตามระดับความเสี่ยงและอยู่ภายใต้การกำกับดูแลที่เหมาะสม เพื่อให้สามารถบริหารจัดการความเสี่ยงที่อาจส่งผลกระทบต่อข้อมูล ระบบงาน ผู้ใช้บริการ ผู้ป่วย และองค์กรได้อย่างมีประสิทธิผล

10.6.1 องค์กรต้องกำหนดให้ระบบ AI หรือบริการ AI ที่ได้รับจากผู้ให้บริการภายนอกอยู่ภายใต้การกำกับดูแลและการบริหารจัดการความเสี่ยงตามกรอบการกำกับดูแลระบบ AI ขององค์กร โดยกำหนดมาตรการควบคุมที่เหมาะสมตามลักษณะการใช้งาน ระดับความเสี่ยง ผลกระทบที่อาจเกิดขึ้น และระดับการพึ่งพาผู้ให้บริการภายนอก

10.6.2 องค์กรต้องกำหนดให้การคัดเลือก การจัดหา และการนำระบบ AI หรือบริการ AI จากผู้ให้บริการภายนอกมาใช้งาน อยู่ภายใต้การประเมินความเสี่ยงก่อนการใช้งานตามระดับความเสี่ยงและลักษณะการใช้งาน โดยครอบคลุมประเด็นด้านจริยธรรม ความโปร่งใส ความมั่นคงปลอดภัย การคุ้มครองข้อมูล ความน่าเชื่อถือ การปฏิบัติตามกฎหมาย ความต่อเนื่องทางธุรกิจ และความสามารถในการกำกับดูแลและบริหารจัดการความเสี่ยงขององค์กรตามความเหมาะสม

10.6.3 องค์กรอาจกำหนดรายชื่อผู้ให้บริการ AI ที่ผ่านการประเมินและได้รับอนุมัติ (Approved / Trusted Providers) เพื่อใช้เป็นแนวทางในการเลือกใช้บริการ ทั้งนี้ การใช้บริการจากผู้ให้บริการที่อยู่นอกบัญชีรายชื่อต้องได้รับการประเมินความเสี่ยงและอนุมัติตามกระบวนการที่กำหนด

10.6.4 องค์กรต้องกำหนดให้สัญญาหรือข้อตกลงกับผู้ให้บริการ AI ครอบคลุมข้อกำหนดที่เกี่ยวข้องกับการบริหารความเสี่ยงและการกำกับดูแลอย่างเหมาะสม ซึ่งอาจรวมถึงขอบเขตการใช้งาน ระดับการให้บริการ การคุ้มครองข้อมูล ความมั่นคงปลอดภัย สิทธิในการตรวจสอบ การแจ้งเหตุการณ์สำคัญ การใช้ผู้รับช่วงงาน และเงื่อนไขการยุติหรือเปลี่ยนผ่านบริการ

10.6.5 องค์กรต้องกำหนดให้มีการรวบรวม พิจารณา และประเมินข้อมูลที่เกี่ยวข้องกับระบบ AI จากผู้ให้บริการภายนอกตามข้อมูลที่องค์กรสามารถได้รับหรือเข้าถึงได้ตามสมควร เพื่อสนับสนุนการกำกับดูแล การบริหารจัดการความเสี่ยง และการใช้งานระบบ AI อย่างเหมาะสม ทั้งนี้ข้อมูลดังกล่าวอาจรวมถึงข้อจำกัด สมมติฐาน ขีดความสามารถ เงื่อนไขการใช้งาน หรือข้อมูลอื่นที่เกี่ยวข้องตามความเหมาะสม

10.6.6 องค์กรต้องกำหนดให้ข้อมูลที่เกี่ยวข้องกับการใช้งานระบบ AI จากผู้ให้บริการภายนอกอยู่ภายใต้การกำกับดูแลและการคุ้มครองข้อมูลตามนโยบายและข้อกำหนดขององค์กร โดยคำนึงถึงการควบคุมการเข้าถึง การใช้ข้อมูลตามวัตถุประสงค์ การจัดเก็บและการเก็บรักษาข้อมูล การเปิดเผยหรือการโอนข้อมูล และความเสี่ยงที่เกี่ยวข้อง

10.6.7 องค์กรต้องกำหนดให้การใช้งานระบบ AI จากผู้ให้บริการภายนอกอยู่ภายใต้การกำกับดูแลโดยมนุษย์ (Human Oversight) ตามระดับความเสี่ยง ลักษณะการใช้งาน แลผลกระทบที่อาจเกิดขึ้น โดยเฉพาะกรณีที่ระบบมีผลต่อการตัดสินใจที่มีนัยสำคัญต่อผู้ใช้ ผู้รับบริการ ผู้ป่วย หรือองค์กร

10.6.8 องค์กรต้องกำหนดให้มีการติดตาม ตรวจสอบ และประเมินผลการใช้งานระบบ AI จากผู้ให้บริการภายนอกอย่างสม่ำเสมอ โดยให้สอดคล้องกับลักษณะการใช้งาน ระดับความเสี่ยง และผลกระทบของระบบ เพื่อให้มั่นใจว่าการใช้บริการยังคงเป็นไปตามวัตถุประสงค์ สัญญา และกรอบการกำกับดูแลขององค์กร

10.6.9 องค์กรต้องกำหนดให้มีการติดตามและประเมินความถูกต้อง ความเหมาะสม ความสม่ำเสมอ และความน่าเชื่อถือของผลลัพธ์จากระบบ AI ของผู้ให้บริการภายนอกอย่างเหมาะสมตามระดับความเสี่ยง ทั้งนี้ แม้องค์กรจะมีการใช้หรือบูรณาการระบบ AI จากผู้ให้บริการภายนอก ความรับผิดชอบต่อการตัดสินใจ ผลลัพธ์ และผลกระทบที่เกิดขึ้นจากการใช้งานระบบ AI ยังคงเป็นความรับผิดชอบขององค์กรและผู้มีอำนาจตัดสินใจตามโครงสร้างการกำกับดูแลขององค์กร

10.6.10 องค์กรต้องกำหนดให้มีการประเมินความเสี่ยงจากการพึ่งพาผู้ให้บริการภายนอก และกำหนดมาตรการรองรับที่เหมาะสม เช่น ความสามารถในการเปลี่ยนผู้ให้บริการ การถ่ายโอนข้อมูล การคืนทรัพย์สินข้อมูล แผนทางเลือกสำรอง และการดำเนินงานต่อเนื่องเมื่อเกิดการหยุดชะงักของบริการ

10.6.11 องค์กรต้องกำหนดให้มีการทบทวนความเสี่ยงของผู้ให้บริการภายนอกเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงบริการ เทคโนโลยี แบบจำลอง โครงสร้างองค์กร สถานะทางการเงิน หรือข้อกำหนดทางกฎหมาย เพื่อให้การกำกับดูแลและการใช้บริการยังคงอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้

10.7 **ความโปร่งใสและการเปิดเผยข้อมูลการใช้งานระบบปัญญาประดิษฐ์** (AI Transparency and Disclosure)

องค์กรต้องจัดให้มีกรอบการกำกับดูแลด้านความโปร่งใส การสื่อสาร และการเปิดเผยข้อมูลเกี่ยวกับระบบ AI อย่างเหมาะสม โดยคำนึงถึงระดับความเสี่ยง วัตถุประสงค์ทางธุรกิจ กฎหมาย ข้อกำหนด และความคาดหวังของผู้มีส่วนได้ส่วนเสีย

10.7.1 องค์กรต้องกำหนดหลักเกณฑ์ ขอบเขต และระดับของการสื่อสารหรือการเปิดเผยข้อมูลเกี่ยวกับระบบ AI ให้เหมาะสมกับลักษณะการใช้งาน ระดับความเสี่ยง และผลกระทบที่อาจเกิดขึ้น โดยคำนึงถึงข้อกำหนดด้านความมั่นคงปลอดภัย ความลับทางธุรกิจ และสิทธิของผู้มีส่วนได้ส่วนเสีย

10.7.2 องค์กรต้องส่งเสริมการสื่อสารภายในองค์กรเกี่ยวกับวัตถุประสงค์ ขอบเขตการใช้งาน ความเสี่ยง ข้อจำกัด และแนวทางการกำกับดูแลระบบ AI เพื่อสนับสนุนความเข้าใจและการปฏิบัติที่สอดคล้องกันทั่วทั้งองค์กร

10.7.3 องค์กรต้องกำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องได้รับข้อมูลที่เพียงพอเกี่ยวกับวัตถุประสงค์ ขอบเขตการใช้งาน ข้อจำกัด ความเสี่ยง และข้อควรระวังของระบบ AI เพื่อสนับสนุนการใช้งานอย่างเหมาะสมและมีความรับผิดชอบ

10.7.4 องค์กรต้องกำหนดแนวทางการเปิดเผยข้อมูลเกี่ยวกับการใช้งานระบบ AI ต่อผู้มีส่วนได้ส่วนเสียภายนอกตามความเหมาะสม โดยคำนึงถึงลักษณะการใช้งาน ระดับความเสี่ยง ผลกระทบที่อาจเกิดขึ้น และข้อกำหนดที่เกี่ยวข้อง

10.7.5 องค์กรต้องกำหนดให้สามารถอธิบายผลลัพธ์ การตัดสินใจ หรือการทำงานของระบบ AI ได้ในระดับที่เหมาะสมกับลักษณะการใช้งาน ความซับซ้อน และระดับความเสี่ยงของระบบ

10.7.6 องค์กรต้องกำกับดูแลให้การสื่อสารเกี่ยวกับระบบ AI มีความถูกต้อง ชัดเจน และไม่ก่อให้เกิดความเข้าใจคลาดเคลื่อนเกี่ยวกับบทบาท ความสามารถ ข้อจำกัด หรือระดับการพึ่งพาระบบ AI

10.7.7 องค์กรต้องกำหนดบทบาท หน้าที่ และความรับผิดชอบในการรายงานหรือเปิดเผยข้อมูลเกี่ยวกับระบบ AI ต่อหน่วยงานกำกับดูแล คู่ค้า ลูกค้า หรือบุคคลภายนอก ตามข้อกำหนดทางกฎหมาย สัญญา และกรอบการกำกับดูแลที่เกี่ยวข้อง

10.7.8 องค์กรต้องจัดให้มีช่องทางที่เหมาะสมสำหรับการสอบถาม ให้ข้อเสนอแนะ หรือรายงานข้อกังวลที่เกี่ยวข้องกับการใช้งานระบบ AI พร้อมกำหนดกระบวนการตอบสนองและติดตามผลตามความเหมาะสม

10.7.9 องค์กรต้องกำหนดแนวทางการสื่อสารเหตุการณ์ ความผิดพลาด หรือประเด็นที่เกี่ยวข้องกับระบบ AI ที่อาจส่งผลกระทบต่อผู้มีส่วนได้ส่วนเสีย โดยต้องดำเนินการอย่างเหมาะสม ทันท่วงที และสอดคล้องกับกระบวนการบริหารจัดการเหตุการณ์ขององค์กร

10.8 **การใช้งานระบบปัญญาประดิษฐ์อย่างมีความรับผิดชอบและมีจริยธรรม** (Responsible and Ethical AI)

องค์กรต้องกำหนด ส่งเสริม และกำกับดูแลให้การพัฒนา การจัดหา และการใช้งานระบบ AI เป็นไปอย่างมีความรับผิดชอบ โปร่งใส เป็นธรรม และสอดคล้องกับค่านิยมองค์กร หลักจริยธรรม และข้อกำหนดที่เกี่ยวข้อง โดยคำนึงถึงผลกระทบต่อผู้มีส่วนได้เสียตลอดวงจรชีวิตของระบบ

10.8.1 องค์กรต้องกำหนดหลักการ นโยบาย หรือแนวปฏิบัติด้าน Responsible AI เพื่อใช้เป็นกรอบในการพัฒนา การจัดหา การใช้งาน และการกำกับดูแลระบบ AI ให้สอดคล้องกับค่านิยมองค์กร หลักธรรมาภิบาล และระดับความเสี่ยงที่องค์กรยอมรับได้

10.8.2 องค์กรต้องกำกับดูแลให้การใช้งานระบบ AI เป็นไปตามวัตถุประสงค์ ขอบเขต และบริบทที่ได้รับอนุมัติ รวมถึงต้องมีมาตรการป้องกันการใช้งานที่ไม่เหมาะสม การใช้งานนอกขอบเขต หรือการใช้งานที่อาจขัดต่อหลักจริยธรรม กฎหมาย หรือข้อกำหนดขององค์กร

10.8.3 องค์กรต้องกำหนดมาตรการที่เหมาะสมเพื่อป้องกัน ตรวจจับ ติดตาม และลดความเสี่ยงจากความลำเอียง (Bias) การเลือกปฏิบัติ การละเมิดสิทธิ หรือผลกระทบเชิงลบที่อาจเกิดขึ้นต่อบุคคลหรือกลุ่มบุคคล โดยเฉพาะกลุ่มเปราะบางหรือผู้ที่อาจได้รับผลกระทบอย่างมีนัยสำคัญ

10.8.4 องค์กรต้องส่งเสริมให้ระบบ AI มีความโปร่งใส สามารถอธิบายได้ในระดับที่เหมาะสมกับลักษณะการใช้งานและระดับความเสี่ยง รวมถึงต้องสามารถกำหนดความรับผิดชอบต่อผลลัพธ์ การตัดสินใจ และผลกระทบที่เกิดขึ้นจากระบบ AI ได้อย่างเหมาะสม

10.8.5 องค์กรต้องพิจารณาและบริหารจัดการผลกระทบที่อาจเกิดขึ้นจากการใช้งานระบบ AI ต่อผู้ใช้ ผู้รับบริการ ผู้ป่วย พนักงาน ผู้มีส่วนได้เสีย และสังคมโดยรวม รวมถึงต้องมีมาตรการป้องกัน บรรเทา และจัดการผลกระทบเชิงลบตามความเหมาะสมและระดับความเสี่ยง

11. การพัฒนาศักยภาพและขีดความสามารถด้านปัญญาประดิษฐ์ (Capabilities and Competency Development)

องค์กรต้องกำหนดและคงไว้ซึ่งการพัฒนาศักยภาพ ความรู้ ขีดความสามารถ และความตระหนักรู้ด้านระบบ AI อย่างต่อเนื่องและสอดคล้องกับระดับความเสี่ยง เพื่อสนับสนุนการพัฒนา การใช้งาน การกำกับดูแล และการบริหารจัดการระบบ AI ให้เป็นไปตามวัตถุประสงค์ทางธุรกิจ หลักธรรมาภิบาล กฎหมาย ข้อกำหนด และนโยบายที่เกี่ยวข้องขององค์กร

11.1 องค์กรต้องกำหนดให้บุคลากรที่เกี่ยวข้องกับระบบ AI มีความรู้ ความสามารถ ประสบการณ์ และคุณสมบัติที่เหมาะสมกับบทบาทหน้าที่ โดยครอบคลุมด้านเทคนิค การบริหารจัดการความเสี่ยง ความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล จริยธรรม กฎหมาย และข้อกำหนดที่เกี่ยวข้องตามความเหมาะสมของหน้าที่รับผิดชอบ

11.2 องค์กรต้องส่งเสริมให้บุคลากรที่เกี่ยวข้องมีความตระหนักและความเข้าใจเกี่ยวกับการใช้งานระบบ AI และความเสี่ยงที่เกี่ยวข้องตามบทบาทหน้าที่ ลักษณะการใช้งาน และระดับความเสี่ยงของระบบ

11.3 องค์กรต้องกำหนดให้ผู้มีอำนาจตัดสินใจหรือผู้กำกับดูแลระบบ AI มีความเข้าใจที่เพียงพอเกี่ยวกับวัตถุประสงค์ ความเสี่ยง ข้อจำกัด และภาระหน้าที่ในการกำกับดูแลระบบ AI เพื่อสนับสนุนการตัดสินใจและการกำกับดูแลอย่างเหมาะสม

11.4 องค์กรต้องจัดให้มีกระบวนการสื่อสารและเผยแพร่ข้อมูลที่เกี่ยวข้องกับระบบ AI และระบบการบริหารจัดการปัญญาประดิษฐ์ (AI Management System: AIMS) ภายในองค์กรอย่างเหมาะสม เพื่อสนับสนุนความเข้าใจ การปฏิบัติตามนโยบาย และการดำเนินงานที่เกี่ยวข้องกับระบบ AI

11.5 องค์กรต้องกำหนดให้มีการประเมินความต้องการด้านทักษะ การวางแผนและดำเนินการฝึกอบรม การติดตามและทบทวนประสิทธิผลของการพัฒนาศักยภาพ รวมถึงกิจกรรมสร้างความตระหนักรู้ด้านระบบ AI อย่างต่อเนื่อง เพื่อให้บุคลากรสามารถปฏิบัติงานและกำกับดูแลระบบ AI ได้อย่างเหมาะสม สอดคล้องกับบริบทการดำเนินงาน ระดับความเสี่ยง และการเปลี่ยนแปลงที่เกี่ยวข้อง

11.6 องค์กรต้องส่งเสริมให้มีการพัฒนา ทบทวน และปรับปรุงองค์ความรู้ ทักษะ และขีดความสามารถด้านระบบ AI ของบุคลากรและผู้ที่เกี่ยวข้องอย่างต่อเนื่อง เพื่อรองรับการเปลี่ยนแปลงของเทคโนโลยี แนวโน้มความเสี่ยง กฎหมาย มาตรฐานอุตสาหกรรม และข้อกำหนดที่เกี่ยวข้อง

12. การติดตาม ตรวจสอบและประเมินผล (Monitoring and Evaluation)

องค์กรต้องกำหนดและคงไว้ซึ่งกระบวนการติดตาม ตรวจสอบ และประเมินผลระบบบริหารจัดการปัญญาประดิษฐ์ (AI Management System: AIMS) และระบบ AI อย่างเป็นระบบและสอดคล้องกับระดับความเสี่ยง เพื่อให้มั่นใจว่าการกำกับดูแล การบริหารจัดการความเสี่ยง มาตรการควบคุม และการใช้งานระบบ AI ยังคงมีความเหมาะสม มีประสิทธิผล และสอดคล้องกับนโยบาย วัตถุประสงค์ทางธุรกิจ ระดับความเสี่ยงที่องค์กรยอมรับได้ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง รวมถึงสนับสนุนการปรับปรุงอย่างต่อเนื่อง

12.1 องค์กรต้องกำหนดให้มีการติดตามและประเมินประสิทธิผลของระบบ AI และระบบบริหารจัดการ AI อย่างเหมาะสม โดยใช้ตัวชี้วัดผลการดำเนินงาน (Key Performance Indicators: KPIs) ตัวชี้วัดความเสี่ยง (Key Risk Indicators: KRIs) หรือเกณฑ์ประเมินอื่นที่เหมาะสม สอดคล้องกับลักษณะการใช้งาน ระดับความเสี่ยง และผลกระทบของระบบ เพื่อสนับสนุนการประเมินประสิทธิผล ความน่าเชื่อถือ แนวโน้มความเสี่ยง และความสอดคล้องของระบบ AI อย่างต่อเนื่อง

12.2 องค์กรต้องดำเนินการประเมินความเหมาะสม ความเพียงพอ และประสิทธิผลของระบบบริหารจัดการ AI และมาตรการควบคุมที่เกี่ยวข้องเป็นระยะ เพื่อให้มั่นใจว่าระบบบริหารจัดการ AI และมาตรการควบคุมยังคงมีความเหมาะสม เพียงพอ และมีประสิทธิผล สอดคล้องกับวัตถุประสงค์ทางธุรกิจ ระดับความเสี่ยงที่องค์กรยอมรับได้ และข้อกำหนดที่เกี่ยวข้อง

12.3 องค์กรต้องกำหนดและดำเนินการตรวจประเมินภายใน (Internal Audit / Internal Assessment) สำหรับระบบบริหารจัดการ AI และการกำกับดูแลระบบ AI อย่างเป็นระบบ ตามแผนงานที่กำหนดและบนพื้นฐานความเสี่ยง โดยผู้ตรวจประเมินต้องมีความเป็นอิสระจากกิจกรรมที่ถูกตรวจ และมีความรู้ ความสามารถ หรือความเชี่ยวชาญที่เหมาะสม เพื่อให้การประเมินเป็นไปอย่างเป็นกลาง น่าเชื่อถือ และสามารถยืนยันความสอดคล้องกับนโยบาย ข้อกำหนด มาตรฐาน และมาตรการควบคุมที่เกี่ยวข้องได้

12.4 องค์กรต้องกำหนดให้ผลการติดตาม การประเมิน และการตรวจประเมินภายในได้รับการบันทึก วิเคราะห์ รายงาน และยกระดับต่อผู้บริหาร คณะกรรมการ หรือหน่วยงานที่เกี่ยวข้องตามระดับความสำคัญของประเด็นความเสี่ยง พร้อมทั้งนำผลดังกล่าวไปใช้ในการปรับปรุงและพัฒนาระบบบริหารจัดการ AI และมาตรการควบคุมอย่างต่อเนื่อง

12.5 องค์กรต้องจัดให้มีการทบทวนระบบบริหารจัดการ AI โดยฝ่ายบริหารหรือผู้บริหารในระดับที่เหมาะสมอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบบริหารจัดการ AI ยังคงมีความเหมาะสม เพียงพอ และมีประสิทธิผล ทั้งนี้ การทบทวนต้องพิจารณาข้อมูลจากผลการติดตาม การประเมิน การตรวจประเมินภายใน เหตุการณ์ด้านความเสี่ยง ข้อร้องเรียน การเปลี่ยนแปลงของบริบทธุรกิจ เทคโนโลยี กฎหมาย และข้อกำหนดที่เกี่ยวข้อง รวมถึงโอกาสในการปรับปรุงและพัฒนาระบบ AI ขององค์กรอย่างต่อเนื่อง

13. **การปรับปรุงและการดำเนินการแก้ไข** (Improvement and Corrective Actions)

องค์กรต้องกำหนดและคงไว้ซึ่งกระบวนการปรับปรุงและการดำเนินการแก้ไขสำหรับระบบบริหารจัดการปัญญาประดิษฐ์ (AI Management System: AIMS) และระบบ AI อย่างเป็นระบบและสอดคล้องกับระดับความเสี่ยง เพื่อสนับสนุนการปรับปรุงระบบบริหารจัดการ AI และมาตรการควบคุมอย่างต่อเนื่อง รวมถึงรองรับการเปลี่ยนแปลงของเทคโนโลยี ความเสี่ยง กฎหมาย มาตรฐาน และบริบทการดำเนินงานขององค์กรอย่างเหมาะสม

13.1 องค์กรต้องกำหนดให้มีการระบุ บันทึก ประเมิน และจัดการกรณีความไม่สอดคล้อง (Nonconformities) ที่เกี่ยวข้องกับระบบ AI อย่างเป็นระบบ โปร่งใส และเหมาะสมตามระดับความเสี่ยงและความรุนแรงของประเด็น เพื่อสนับสนุนการจัดการและลดผลกระทบต่อผู้มีส่วนได้เสีย การดำเนินงาน การปฏิบัติตามข้อกำหนด และชื่อเสียงขององค์กรอย่างทันท่วงที

13.2 องค์กรต้องกำหนดให้มีการดำเนินการแก้ไข (Corrective Actions) ต่อความไม่สอดคล้องหรือเหตุการณ์ที่เกี่ยวข้องกับระบบ AI อย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยง สาเหตุที่แท้จริง (Root Cause) และผลกระทบของประเด็นที่เกิดขึ้น ทั้งนี้ การดำเนินการแก้ไขต้องอยู่ภายใต้การกำกับดูแล การติดตามผล และการทบทวนตามกระบวนการและระดับอำนาจหน้าที่ที่องค์กรกำหนด

13.3 องค์กรต้องจัดให้มีการปรับปรุงระบบบริหารจัดการ AI และมาตรการควบคุมอย่างต่อเนื่อง (Continual Improvement) โดยอ้างอิงจากผลการติดตามและประเมินผล การตรวจประเมินภายใน เหตุการณ์ ความไม่สอดคล้อง ข้อร้องเรียน บทเรียนที่ได้รับ แนวโน้มความเสี่ยง และการเปลี่ยนแปลงของบริบทการดำเนินงาน เพื่อให้ระบบ AI ยังคงมีความเหมาะสม มีประสิทธิผล และสอดคล้องกับข้อกำหนดที่เกี่ยวข้อง

13.4 องค์กรต้องกำหนดให้มีการจัดทำ จัดเก็บ และคงรักษาบันทึกที่เกี่ยวข้องกับความไม่สอดคล้อง การวิเคราะห์สาเหตุ การดำเนินการแก้ไข ผลการติดตาม และกิจกรรมการปรับปรุงอย่างเหมาะสม เพื่อสนับสนุนการกำกับดูแล การตรวจสอบภายใน การตรวจประเมิน และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง

14. การนำนโยบายไปใช้และบทเฉพาะกาล (Policy Implementation and Transitional Provisions)

เพื่อให้การนำนโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์ไปใช้เป็นไปอย่างมีประสิทธิผล สอดคล้องกับระดับความเสี่ยง และสามารถดำเนินการได้ในทางปฏิบัติ บริษัทกำหนดแนวทางการเปลี่ยนผ่านสำหรับระบบ AI ที่มีการพัฒนา จัดหา บูรณาการ หรือใช้งานอยู่ก่อนวันที่นโยบายมีผลบังคับใช้ รวมถึงกำหนดหลักเกณฑ์ในการดำเนินการเพิ่มเติมสำหรับระบบ AI ที่มีความเสี่ยงสูงหรือมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้การเปลี่ยนผ่านสู่การกำกับดูแลระบบ AI เป็นไปอย่างเหมาะสมตามระดับความเสี่ยงและบริบทการดำเนินงานขององค์กร

14.1 ระบบปัญญาประดิษฐ์ที่อยู่ในขอบเขตของนโยบายฉบับนี้และมีการพัฒนา จัดหา บูรณาการ หรือใช้งานอยู่ก่อนวันที่นโยบายมีผลบังคับใช้ ต้องได้รับการทบทวน ประเมิน และดำเนินการให้สอดคล้องกับข้อกำหนดของนโยบายฉบับนี้ตามระดับความเสี่ยง ลักษณะการใช้งาน และระยะเวลาที่บริษัทกำหนด

14.2 บริษัทอาจกำหนดแนวทาง ระยะเวลา มาตรการควบคุมเพิ่มเติม ข้อยกเว้น หรือมาตรการผ่อนผันที่เหมาะสมสำหรับระบบ AI ที่มีอยู่เดิม โดยคำนึงถึงระดับความเสี่ยง ผลกระทบ ความพร้อมขององค์กร และข้อจำกัดในการดำเนินงานตามความเหมาะสม

14.3 สำหรับระบบ AI ที่มีความเสี่ยงสูง หรือเกี่ยวข้องกับข้อมูลสุขภาพ ข้อมูลส่วนบุคคล ข้อมูลสำคัญขององค์กร หรือกระบวนการที่มีนัยสำคัญต่อผู้ป่วย ผู้รับบริการ หรือองค์กร บริษัทอาจกำหนดให้มีการทบทวน ประเมิน และดำเนินการให้สอดคล้องกับนโยบายฉบับนี้เป็นลำดับแรกตามความเหมาะสม

15. การบังคับใช้ (Enforcement)

นโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์ (AI Governance Policy) ฉบับนี้ถือเป็นข้อกำหนดบังคับขององค์กร ซึ่งคณะกรรมการ ผู้บริหาร พนักงาน ผู้รับจ้าง ผู้ให้บริการ คู่ค้า และบุคคลภายนอกที่เกี่ยวข้องกับการพัฒนา การจัดหา การบูรณาการ การกำกับดูแล หรือการใช้งานระบบ AI ในนามขององค์กร ต้องปฏิบัติตามอย่างเคร่งครัด ทั้งนี้ การดำเนินงานที่เกี่ยวข้องกับระบบ AI ต้องสอดคล้องกับหลักธรรมาภิบาล ความรับผิดชอบ ความโปร่งใส ความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล จริยธรรม กฎหมาย และระดับความเสี่ยงที่องค์กรยอมรับได้

15.1 องค์กรต้องกำหนดและมอบหมายหน่วยงาน คณะกรรมการ หรือผู้มีอำนาจที่เหมาะสม ให้รับผิดชอบในการกำกับดูแล ติดตาม ประเมิน และรายงานผลการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์ อย่างสม่ำเสมอ รวมถึงมีอำนาจเสนอแนะ สั่งการ หรือกำหนดมาตรการแก้ไขเมื่อพบการไม่ปฏิบัติตามข้อกำหนด หรือเมื่อพบความเสี่ยงที่อาจส่งผลกระทบต่อองค์กรหรือผู้มีส่วนได้เสีย

15.2 การไม่ปฏิบัติตามนโยบายนี้ รวมถึงการพัฒนา การจัดหา การใช้งาน หรือการเปลี่ยนแปลงระบบ AI โดยไม่ได้รับอนุมัติ การหลีกเลี่ยงมาตรการควบคุม การใช้งาน AI ในลักษณะที่ไม่เหมาะสม หรือการดำเนินการที่อาจก่อให้เกิดความเสี่ยงต่อผู้มีส่วนได้ส่วนเสีย ข้อมูล ระบบงาน หรือองค์กร ถือเป็นการฝ่าฝืนข้อกำหนดขององค์กร และอาจนำไปสู่การ

ดำเนินการทางวินัย ทางปกครอง ทางแพ่ง หรือทางกฎหมาย ตามข้อบังคับ ระเบียบ สัญญา และกฎหมายที่เกี่ยวข้อง โดยพิจารณาตามระดับความร้ายแรง เจตนา ความเสียหาย และผลกระทบของการกระทำ

15.3 ในกรณีที่ผู้รับจ้าง ผู้ให้บริการ คู่ค้า หรือบุคคลภายนอกไม่ปฏิบัติตามข้อกำหนดด้านด้านการกำกับดูแลและบริหารจัดการปัญญาประดิษฐ์ หรือข้อกำหนดตามสัญญาที่เกี่ยวข้อง องค์กรมีสิทธิ์ดำเนินการตามเงื่อนไขที่กำหนดไว้ ซึ่งอาจรวมถึงการกำหนดแผนแก้ไข การจำกัดหรือระงับสิทธิ์การเข้าถึง การระงับการให้บริการ การเรียกค่าเสียหาย การบอกเลิกสัญญา หรือการดำเนินการทางกฎหมายตามความเหมาะสมและระดับความเสี่ยงของเหตุการณ์

15.4 องค์กรต้องจัดให้มีช่องทางที่เหมาะสม ปลอดภัย และเป็นความลับ สำหรับการรายงานเหตุการณ์ การใช้งานระบบ AI ที่ไม่เหมาะสม การฝ่าฝืนนโยบาย หรือพฤติกรรมที่อาจก่อให้เกิดความเสี่ยง พร้อมทั้งต้องคุ้มครองผู้แจ้งเบาะแส (Whistleblower) จากการกลั่นแกล้ง การตอบโต้ หรือการเลือกปฏิบัติ และดำเนินการตรวจสอบข้อร้องเรียนหรือรายงานดังกล่าวอย่างเป็นธรรม ทันท่วงที และเหมาะสม โดยสอดคล้องกับนโยบายและกระบวนการบริหารจัดการข้อร้องเรียนหรือการแจ้งเบาะแสขององค์กรที่เกี่ยวข้อง

16. เอกสารที่เกี่ยวข้อง (Related Documents)

1. SP-03-BDMS-021 กรอบบริหารความเสี่ยงองค์กร บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
2. WP-03-BDMS-018 ขั้นตอนการบริหารความเสี่ยง บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
3. SP-06-BDMS-004-TH นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy)
4. SP-06-BDMS-005-TH นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy)
5. SP-06-BDMS-006-TH นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Policy)
6. WP-06-BDMS-002-TH ขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Procedure)
7. WP-06-BDMS-006-TH ขั้นตอนปฏิบัติการจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management Procedure)
8. WP-06-BDMS-008-TH ขั้นตอนปฏิบัติการบริหารจัดการบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ (IT Third-Party Management Procedure)

17. ภาคผนวก (Annex)

ภาคผนวก A: แนวทางการกำกับดูแลระบบปัญญาประดิษฐ์ตามระดับความเสี่ยง

ภาคผนวกนี้จัดทำขึ้นเพื่อเป็นแนวทางอ้างอิงสำหรับการกำกับดูแล การควบคุม และการบริหารจัดการความเสี่ยงของระบบปัญญาประดิษฐ์ (Artificial Intelligence Systems: AI Systems) ตามระดับความเสี่ยง เพื่อสนับสนุนให้หน่วยงานและผู้ที่เกี่ยวข้องสามารถพิจารณา กำกับดูแล และกำหนดมาตรการควบคุมที่เหมาะสม สอดคล้องกับลักษณะการใช้งาน ผลกระทบ และระดับความเสี่ยงของระบบ AI ได้อย่างเหมาะสมและสอดคล้องทั่วทั้งองค์กร

แนวทางในภาคผนวกนี้เป็นการสรุปข้อกำหนดและแนวปฏิบัติในระดับภาพรวม และไม่ถือเป็นการกำหนดข้อกำหนดเพิ่มเติมนอกเหนือจากที่ระบุไว้ในนโยบาย โดยจัดกลุ่มตามระดับความเสี่ยงของระบบ AI เพื่อสนับสนุนการนำกรอบธรรมาภิบาล การบริหารจัดการความเสี่ยง และมาตรการควบคุมไปประยุกต์ใช้ตามหลักการกำกับดูแลตามระดับความเสี่ยง (Risk-Based Governance) และสอดคล้องกับบริบทการดำเนินงานขององค์กร

ระดับความเสี่ยงของระบบ AI	แนวทางในการกำกับดูแล
1. ระบบ AI ที่มีความเสี่ยงที่ไม่อาจยอมรับได้ (Unacceptable Risk AI Systems)	- ห้ามพัฒนา จัดหา นำไปใช้ หรือใช้งาน เว้นแต่ได้รับอนุญาตตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้องโดยเฉพาะ - ต้องมีกลไกการคัดกรองและประเมินกรณีการใช้งาน (Use Case Assessment) ก่อนการพัฒนา จัดหา หรือนำไปใช้ เพื่อป้องกันความเสี่ยงที่ไม่อาจยอมรับได้ - ต้องมีกลไกในการตรวจสอบ ติดตาม ระงับ หรือยุติการใช้งานตามความเหมาะสมและความเร่งด่วนของความเสี่ยง หากพบว่าระบบไม่สอดคล้องกับกฎหมาย หลักจริยธรรม ข้อกำหนดขององค์กร หรือก่อให้เกิดความเสี่ยงในระดับที่ไม่อาจยอมรับได้ - ต้องมีการยกระดับและรายงานประเด็นต่อผู้บริหารระดับสูงหรือคณะกรรมการที่เกี่ยวข้องโดยไม่ชักช้า - ต้องจัดเก็บข้อมูล เอกสาร และหลักฐานที่เกี่ยวข้องอย่างเหมาะสม เพื่อรองรับการตรวจสอบย้อนหลังและการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง
2. ระบบ AI ระดับความเสี่ยงสูง (High Risk AI Systems)	- ต้องอยู่ภายใต้การกำกับดูแลโดยผู้มีอำนาจตามระดับที่องค์กรกำหนด - ต้องดำเนินการประเมินความเสี่ยงและการประเมินผลกระทบของระบบปัญญาประดิษฐ์ (AI Impact Assessment) หรือพิจารณาผลการประเมินที่เกี่ยวข้องจากผู้ให้บริการภายนอกตามความเหมาะสม ก่อนการพัฒนา จัดหา นำไปใช้ และอย่างต่อเนื่องตลอดวงจรชีวิตของระบบ - ต้องกำหนดมาตรการควบคุม การกำกับดูแล และการติดตามที่เหมาะสม สอดคล้องกับระดับความเสี่ยงและผลกระทบของระบบ รวมถึงการกำกับดูแลโดยมนุษย์ตามความเหมาะสม - ต้องมีการติดตาม ตรวจสอบ ทวนสอบ และประเมินผลการทำงานของระบบอย่างต่อเนื่อง รวมถึงการบริหารจัดการความเสี่ยงด้านความเอนเอียงของผลลัพธ์ (Bias) ความมั่นคงปลอดภัย ความน่าเชื่อถือ และผลกระทบต่อผู้มีส่วนได้ส่วนเสีย - ต้องมีกลไกในการรายงานและยกระดับเหตุการณ์ ความเสี่ยง หรือประเด็นสำคัญต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องตามกระบวนการที่กำหนด - ต้องจัดเก็บข้อมูล เอกสาร และหลักฐานที่เกี่ยวข้องอย่างเหมาะสม เพื่อรองรับการตรวจสอบย้อนหลัง การติดตาม และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง
3. ระบบ AI ระดับความเสี่ยงจำกัด (Limited Risk AI Systems)	- ต้องมีความโปร่งใสในการใช้งานระบบ AI อย่างเหมาะสม โดยอาจกำหนดให้มีการแจ้งหรือเปิดเผยต่อผู้ใช้งาน ผู้มีส่วนได้เสีย หรือผู้ที่เกี่ยวข้องให้ทราบว่ามีการใช้ระบบ AI เป็นส่วนหนึ่งของกระบวนการตัดสินใจหรือการให้บริการ ตามบริบท ลักษณะการใช้งาน และระดับความเสี่ยงของระบบ - ต้องมีการประเมินความเสี่ยงหรือผลกระทบของระบบ AI ในระดับที่เหมาะสมกับลักษณะการใช้งาน ระดับความเสี่ยง และผลกระทบของระบบ ทั้งนี้ องค์กรอาจกำหนดแนวทาง มาตรฐาน หรือหลักเกณฑ์เพิ่มเติมสำหรับการประเมินความเสี่ยง การ

ระดับความเสี่ยงของระบบ AI	แนวทางในการกำกับดูแล
	ประเมินผลกระทบ และมาตรการควบคุม ให้เหมาะสมกับบริบททางธุรกิจและลักษณะการใช้งานของแต่ละหน่วยงาน - ต้องกำหนดมาตรการควบคุมเพิ่มเติมตามระดับความเสี่ยงและบริบทของการใช้งาน ซึ่งอาจรวมถึงการควบคุมคุณภาพข้อมูล การกำหนดขอบเขตและเงื่อนไขการใช้งาน การกำกับดูแลโดยมนุษย์ (Human Oversight) การควบคุมสิทธิ์การเข้าถึง และการติดตามผลลัพธ์ของระบบตามความเหมาะสม - ต้องมีการติดตาม ตรวจสอบ และทบทวนคุณภาพผลลัพธ์ รวมถึงความเสี่ยงหรือผลกระทบที่เกี่ยวข้องตามความเหมาะสม - ควรมีกลไกในการรายงานและยกระดับประเด็นตามความเหมาะสม เมื่อพบความเสี่ยง เหตุการณ์ หรือผลลัพธ์ที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อผู้ใช้งาน องค์กร หรือผู้มีส่วนได้เสีย
4. ระบบ AI ระดับความเสี่ยงต่ำหรือความเสี่ยงน้อย (Minimal Risk AI Systems)	- ต้องใช้งานภายใต้มาตรการควบคุมพื้นฐาน (Baseline Controls) ตามนโยบาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้องขององค์กร - ต้องมีมาตรการพื้นฐานด้านความมั่นคงปลอดภัย การคุ้มครองข้อมูล และการใช้งาน AI ที่เหมาะสมกับวัตถุประสงค์และลักษณะการใช้งานของระบบ - ควรมีการติดตามและทบทวนการใช้งาน รวมถึงระดับความเสี่ยงของระบบตามความเหมาะสม และเมื่อมีการเปลี่ยนแปลงลักษณะการใช้งานที่อาจส่งผลกระทบต่อระดับความเสี่ยงของระบบ - ต้องมีกระบวนการยกระดับ เมื่อพบว่าระดับความเสี่ยงของระบบเปลี่ยนแปลง หรือมาตรการควบคุมพื้นฐานที่กำหนดไม่สอดคล้องกับระดับความเสี่ยงของระบบอีกต่อไป

<u>หมายเหตุ</u>

- รายละเอียดของข้อกำหนด มาตรการควบคุม และแนวทางการดำเนินงาน ให้เป็นไปตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติงาน และข้อกำหนดที่เกี่ยวข้องขององค์กรเป็นหลัก
- การกำหนดระดับความเสี่ยงของระบบ AI ควรพิจารณาจากลักษณะการใช้งาน ระดับความเป็นอิสระของระบบ ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย ความสำคัญของกระบวนการทางธุรกิจ และความเสี่ยงที่อาจเกิดขึ้น
- ระดับความเสี่ยงของระบบ AI อาจเปลี่ยนแปลงได้ตามบริบท ข้อมูล วัตถุประสงค์ หรือรูปแบบการใช้งานของระบบ และควรได้รับการทบทวนและประเมินใหม่ตามความเหมาะสมหรือการเปลี่ยนแปลงที่มีนัยสำคัญ
- หน่วยงานเจ้าของระบบและผู้ที่เกี่ยวข้องต้องกำกับดูแลและบริหารจัดการความเสี่ยงของระบบ AI ให้สอดคล้องกับระดับความเสี่ยงที่กำหนดตลอดวงจรชีวิตของระบบ
- กรณีมีการเปลี่ยนแปลงสาระสำคัญ หรือพบเหตุการณ์ ความเสี่ยง หรือผลกระทบที่อาจส่งผลต่อระดับความเสี่ยงของระบบ AI ต้องมีการประเมินระดับความเสี่ยงใหม่ รวมถึงพิจารณาการปรับมาตรการควบคุม ระดับการกำกับดูแล หรืออำนาจการพิจารณาอนุมัติตามกระบวนการที่องค์กรกำหนด

ภาคผนวก B: แนวทางการดำเนินการก่อนการนำระบบปัญญาประดิษฐ์มาใช้ในองค์กร

ภาคผนวกนี้จัดทำขึ้นเพื่อเป็นแนวทางอ้างอิงสำหรับการดำเนินการในระยะก่อนการนำระบบ AI มาใช้ภายในองค์กร โดยมีวัตถุประสงค์เพื่อสนับสนุนให้ผู้ปฏิบัติงานสามารถเตรียมความพร้อมและดำเนินการได้อย่างเป็นระบบ ภายหลังจากที่ได้ทำความเข้าใจนโยบาย หลักเกณฑ์ และมาตรการควบคุมที่เกี่ยวข้องแล้ว ทั้งนี้ แนวทางดังกล่าวเป็นกรอบการดำเนินการในระดับภาพรวม และไม่ถือเป็นการกำหนดข้อกำหนดเพิ่มเติมนอกเหนือจากที่ระบุไว้ในนโยบาย โดยการดำเนินงานต้องเป็นไปตามนโยบาย ระเบียบ มาตรฐาน และข้อกำหนดที่เกี่ยวข้องขององค์กร รวมถึงกฎหมาย กฎระเบียบ และข้อกำหนดภายนอกที่ใช้บังคับ ภายใต้หลักธรรมาภิบาล การบริหารจัดการความเสี่ยง และแนวปฏิบัติสากล

1. ควรมีการระบุและจัดทำทะเบียนระบบปัญญาประดิษฐ์ (AI Inventory) เพื่อรองรับการติดตามและกำกับดูแลระบบ AI ที่อยู่ในขอบเขตตามหลักเกณฑ์ที่บริษัทกำหนด โดยข้อมูลที่จัดเก็บควรมีความเหมาะสม เพียงพอ และเป็นปัจจุบัน ซึ่งอาจครอบคลุมวัตถุประสงค์การใช้งาน เจ้าของระบบ แหล่งข้อมูล ระดับความเสี่ยง ผู้ให้บริการภายนอก (ถ้ามี) และสถานะของระบบ
2. ก่อนการนำระบบ AI มาใช้งาน ควรมีการประเมินความเสี่ยงและผลกระทบของระบบตามกรอบการบริหารจัดการความเสี่ยงที่องค์กรกำหนด รวมถึงการพิจารณาระดับความเสี่ยง การกำหนดมาตรการควบคุมที่เหมาะสม และการพิจารณาอนุมัติตามระดับอำนาจที่เกี่ยวข้อง ก่อนเริ่มใช้งาน
3. ควรมีการพิจารณาความเหมาะสมของข้อมูลที่ใช้กับระบบ AI รวมถึงข้อกำหนดด้านการคุ้มครองข้อมูล ความเป็นส่วนตัว ความมั่นคงปลอดภัย และข้อจำกัดในการใช้ข้อมูลที่เกี่ยวข้อง ก่อนการนำระบบ AI มาใช้งาน
4. สำหรับระบบ AI หรือบริการ AI ที่ได้รับจากผู้ให้บริการภายนอก ควรมีการพิจารณาข้อมูลที่เกี่ยวข้องกับระบบเท่าที่องค์กรสามารถได้รับหรือเข้าถึงได้ตามสมควร รวมถึงการประเมินความเสี่ยงและกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความเสี่ยงและลักษณะการใช้งาน
5. ควรมีการกำหนดบทบาทและความรับผิดชอบของเจ้าของระบบ ผู้ใช้งาน และผู้ที่เกี่ยวข้อง รวมถึงพิจารณาความจำเป็นในการกำกับดูแลโดยมนุษย์ (Human Oversight) ตามระดับความเสี่ยงและผลกระทบของระบบ
6. สำหรับระบบ AI ที่มีการใช้งานอยู่ก่อน (Existing Systems) หรือระบบที่ยังไม่ได้รับการระบุใน AI Inventory ควรมีการดำเนินการระบุ บันทึก ประเมินความเสี่ยง และปรับปรุงให้สอดคล้องกับนโยบายและข้อกำหนดที่เกี่ยวข้องภายในระยะเวลาที่เหมาะสม
7. ในกรณีที่มีความไม่ชัดเจนเกี่ยวกับการจำแนกระบบ การจัดระดับความเสี่ยง การกำหนดมาตรการควบคุม หรือการตีความข้อกำหนดที่เกี่ยวข้อง ควรดำเนินการขอคำปรึกษา หรือยกระดับประเด็นต่อคณะกรรมการกำกับดูแลระบบ AI หรือหน่วยงานที่ได้รับมอบหมายก่อนดำเนินการ

ภาคผนวก C: รายชื่อบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย

1. ธุรกิจโรงพยาบาลเอกชน (Healthcare Business)

   https://investor.bdms.co.th/th/general/bdms-at-a-glance

   20250513-bdms-he
   althcare-business-th

2. ธุรกิจที่เกี่ยวเนื่องกับการรักษาพยาบาล (Business Related to Medical Services)

   https://investor.bdms.co.th/th/general/bdms-at-a-glance

20240313-businessr
elated-to-medicalse

18. เอกสารอ้างอิง (Reference)

1. International Organization for Standardization, & International Electrotechnical Commission. (2022). Artificial intelligence — Artificial intelligence concepts and terminology (ISO/IEC 22989:2022). ISO.
2. International Organization for Standardization, & International Electrotechnical Commission. (2022). Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations (ISO/IEC 38507:2022). ISO.
3. International Organization for Standardization, & International Electrotechnical Commission. (2023). Information technology — Artificial intelligence — Management system (ISO/IEC 42001:2023). ISO.
4. Monetary Authority of Singapore. (2018). Principles to promote fairness, ethics, accountability, and transparency (FEAT) in the use of artificial intelligence and data analytics. MAS.
5. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce.
6. ราชกิจจานุเบกษา. (2562). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. สำนักนายกรัฐมนตรี.
7. ราชกิจจานุเบกษา. (2562). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA). สำนักนายกรัฐมนตรี.
8. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2564). แนวปฏิบัติจริยธรรมปัญญาประดิษฐ์แห่งชาติ (Thailand AI Ethics Guideline).
9. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2568). AI Security Guideline: แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย.