



นโยบายและแนวทางการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัยและมีธรรมาภิบาล

สำนักเลขาธิการนายกรัฐมนตรีให้ความสำคัญกับการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างถูกต้อง เหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัย จึงได้จัดทำนโยบายและแนวทางการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ฉบับนี้ขึ้น เพื่อเป็นกรอบในการดำเนินการและการกำกับดูแลการใช้งาน AI ตลอดจนจรรยาบรรณชีวิตอย่างเป็นระบบ ให้สอดคล้องกับกฎหมายระเบียบ มาตรฐานที่เกี่ยวข้อง และหลักจริยธรรมปัญญาประดิษฐ์ โดยมีรายละเอียด ดังนี้

๑. วัตถุประสงค์

๑.๑ เพื่อให้การพัฒนา การบริหารจัดการ และกำกับดูแลการใช้งาน AI สอดคล้องกับกฎหมายระเบียบ มาตรฐานที่เกี่ยวข้อง และหลักจริยธรรมปัญญาประดิษฐ์

๑.๒ เพื่อกำหนดแนวปฏิบัติในการใช้งาน AI ให้ถูกต้อง เหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัย และเป็นไปตามหลักธรรมาภิบาล ซึ่งจะช่วยป้องกันและลดความเสี่ยงจากการรั่วไหลของข้อมูลสำคัญ ข้อมูลลับ และข้อมูลส่วนบุคคล รวมทั้งสนับสนุนการปฏิบัติงานให้เกิดประสิทธิผลมากยิ่งขึ้น

๑.๓ เพื่อเสริมสร้างความรู้ ความเข้าใจ และความตระหนักรู้ในการใช้งาน AI อย่างมีความรับผิดชอบ

๑.๔ เพื่อส่งเสริมการใช้งาน AI ในการเพิ่มประสิทธิภาพการบริหารราชการ และการตัดสินใจเชิงนโยบาย

๒. ขอบเขต

นโยบายและแนวทางนี้มีผลบังคับใช้กับข้าราชการ ลูกจ้างประจำ พนักงานราชการ และผู้รับจ้างหรือผู้ขายที่เป็นคู่สัญญากับสำนักเลขาธิการนายกรัฐมนตรี โดยครอบคลุมเทคโนโลยีปัญญาประดิษฐ์ทุกประเภทที่สำนักเลขาธิการนายกรัฐมนตรีจัดหาหรืออนุญาตให้นำมาใช้สนับสนุนการดำเนินงานตามภารกิจของสำนักเลขาธิการนายกรัฐมนตรี

๓. คณะกรรมการกำกับดูแลการใช้งานปัญญาประดิษฐ์

คณะกรรมการกำกับดูแลการใช้งานปัญญาประดิษฐ์ของสำนักเลขาธิการนายกรัฐมนตรี มีองค์ประกอบ และหน้าที่และอำนาจ ดังนี้

๓.๑ องค์ประกอบ

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)	ประธานกรรมการ
(๒) ผู้ช่วยเลขาธิการนายกรัฐมนตรี	รองประธานกรรมการ
(๓) ผู้อำนวยการสำนักงาน/กอง/ศูนย์/สำนัก/กลุ่ม/หัวหน้าศูนย์	กรรมการ
(๔) ผู้อำนวยการกลุ่มกฎหมาย	กรรมการ
(๕) ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ	เลขานุการ
(๖) ผู้อำนวยการกลุ่มพัฒนาระบบสารสนเทศนายกรัฐมนตรี	ผู้ช่วยเลขานุการ
(๗) ผู้อำนวยการกลุ่มแผนและการบริหารจัดการระบบเทคโนโลยีสารสนเทศ	ผู้ช่วยเลขานุการ
(๘) ผู้อำนวยการกลุ่มบริหารระบบเครือข่ายและระบบคอมพิวเตอร์	ผู้ช่วยเลขานุการ
(๙) ผู้อำนวยการกลุ่มพัฒนาระบบงานดิจิทัล	ผู้ช่วยเลขานุการ

๓.๒ หน้าที่และอำนาจ

(๑) กำหนดนโยบายและแนวทางการใช้งานปัญญาประดิษฐ์อย่างมีความมั่นคงปลอดภัยและมีธรรมาภิบาล รวมทั้งทบทวนและปรับปรุงให้มีความเหมาะสม สอดคล้องกับสถานการณ์ เทคโนโลยี กฎหมาย และมาตรฐานที่เกี่ยวข้องอยู่เสมอ

(๒) ติดตาม ประเมินผล และกำกับดูแลการปฏิบัติงานให้เป็นไปตามนโยบายและแนวทางการใช้งานปัญญาประดิษฐ์อย่างมีความมั่นคงปลอดภัยและมีธรรมาภิบาล

(๓) บริหารจัดการความเสี่ยงที่เกิดจากการใช้งานปัญญาประดิษฐ์ให้อยู่ในระดับที่ยอมรับได้

(๔) พิจารณาให้ความเห็นชอบการดำเนินการด้านต่าง ๆ ที่เกี่ยวกับการใช้งาน AI ของสำนักเลขาธิการนายกรัฐมนตรี

๔. บทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้อง

ผู้รับผิดชอบ	หน้าที่และความรับผิดชอบ
ระดับนโยบาย (Strategic Level)	
- เลขาธิการนายกรัฐมนตรี - รองเลขาธิการนายกรัฐมนตรีฝ่ายบริหาร หรือข้าราชการที่ได้รับมอบหมายให้กำกับดูแลและปฏิบัติราชการแทนเลขาธิการนายกรัฐมนตรี	กำหนดทิศทาง นโยบายและกำกับดูแล ตลอดจนพิจารณาอนุมัติแนวทางการใช้งานและการดำเนินการเกี่ยวกับปัญญาประดิษฐ์ของสำนักเลขาธิการนายกรัฐมนตรี
ระดับบริหารจัดการ (Management Level)	
คณะกรรมการกำกับดูแลการใช้งานปัญญาประดิษฐ์	- กำหนดนโยบายและแนวทางการใช้งาน AI อย่างมีธรรมาภิบาล รวมทั้งทบทวนและปรับปรุงให้มีความเหมาะสม สอดคล้องกับสถานการณ์ เทคโนโลยี กฎหมาย และมาตรฐานที่เกี่ยวข้องอยู่เสมอ - ติดตาม ประเมินผล และกำกับดูแลการปฏิบัติงานให้เป็นไปตามนโยบายและแนวทางการใช้งาน AI อย่างมีธรรมาภิบาล - บริหารจัดการความเสี่ยงที่เกิดจากการใช้งาน AI ให้อยู่ในระดับที่ยอมรับได้ - พิจารณาให้ความเห็นชอบการดำเนินการด้านต่าง ๆ ที่เกี่ยวกับการใช้งาน AI ของสำนักเลขาธิการนายกรัฐมนตรี
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	- ศึกษา คัดเลือก เครื่องมือ AI ที่เหมาะสมกับภารกิจ - ออกแบบระบบ และการเชื่อมโยง AI เข้ากับระบบงานเดิม - กำกับดูแลการเชื่อมต่อระบบและการเข้าถึงข้อมูลของผู้ให้บริการภายนอก - ดูแลระบบ Log Monitoring และ Incident Response - ติดตามประสิทธิภาพของ AI อย่างสม่ำเสมอ - สนับสนุนการอบรมบุคลากรให้ใช้งาน AI ได้อย่างถูกต้อง

ผู้รับผิดชอบ	หน้าที่และความรับผิดชอบ
ระดับปฏิบัติการ (Operational Level)	
หน่วยงานเจ้าของโครงการ หรือรับผิดชอบภารกิจ (สำนักงาน สำนัก กอง ศูนย์ กลุ่ม)	- เสนอความต้องการใช้ AI ให้สอดคล้องกับภารกิจ - กำหนดวัตถุประสงค์ ขอบเขต และตัวชี้วัดความสำเร็จ - ตรวจสอบคุณภาพข้อมูลที่ให้กับ AI และควบคุมไม่ให้เกิดการรั่วไหลของข้อมูลสำคัญ ข้อมูลลับ และข้อมูลส่วนบุคคล - ควบคุมการใช้งานให้อยู่ในขอบเขตที่อนุมัติ - รับผิดชอบผลลัพธ์จาก AI ที่นำไปใช้ประกอบการปฏิบัติงาน - รายงานปัญหา ความเสี่ยง หรือข้อผิดพลาดต่อผู้บริหาร - ประเมินความคุ้มค่าและผลสัมฤทธิ์ของโครงการ
ผู้ใช้งาน (Users) ได้แก่ ข้าราชการ พนักงานราชการ ลูกจ้างประจำ หรือบุคลากร ที่ได้รับอนุญาตให้ใช้งาน AI	- ปฏิบัติตามนโยบายและแนวทางที่กำหนด - ควบคุมดูแลและใช้ข้อมูลของทางราชการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ - ตรวจสอบความถูกต้อง ครบถ้วน และความเหมาะสมของผลลัพธ์ที่เกิดจากการใช้ AI ก่อนนำไปใช้งานจริง โดยผู้ใช้งานเป็นผู้ตัดสินใจขั้นสุดท้าย - รายงานเหตุผิดปกติอันเกิดจากการใช้งาน AI เช่น ข้อมูลรั่วไหล คำตอบผิดพลาด อคติ หรือความเสี่ยงด้านจริยธรรม - รับผิดชอบการใช้งาน AI ภายใต้บัญชีผู้ใช้ของตนเอง

๕. แนวทางการใช้งาน AI ในภารกิจของสำนักเลขาธิการนายกรัฐมนตรี

สำนักเลขาธิการนายกรัฐมนตรีสามารถนำ AI มาประยุกต์ใช้งานให้เหมาะสมกับลักษณะงานและผลลัพธ์ที่ต้องการ รวมทั้งต้องมีการบริหารจัดการข้อมูลที่จะนำมาใช้งานกับ AI โดยมีรายละเอียดดังนี้

๕.๑ กลยุทธ์การเลือกใช้ AI

หน่วยงานภายในสามารถประยุกต์ใช้ AI ให้เหมาะสมกับลักษณะงานและผลลัพธ์ที่ต้องการ โดยคำนึงถึงข้อจำกัด ความถูกต้อง และความเสี่ยงที่อาจเกิดขึ้น เพื่อยกระดับประสิทธิภาพในการปฏิบัติงาน โดยอาจพิจารณาเลือกใช้ AI ตามตัวอย่างดังต่อไปนี้

(๑) งานด้านวิเคราะห์นโยบายและการสนับสนุนผู้บริหาร โดยการนำ AI มาใช้ในการวิเคราะห์ข้อมูล สรุปสาระสำคัญ จัดทำสรุปนโยบาย เปรียบเทียบนโยบาย วิเคราะห์หรือคาดการณ์แนวโน้มประเด็นสำคัญ และจัดทำรายงานสรุปผู้บริหาร เพื่อเพิ่มประสิทธิภาพในการวิเคราะห์ข้อมูล การจัดทำข้อเสนอเชิงนโยบาย และสนับสนุนการตัดสินใจของผู้บริหาร เช่น Analytics, Large Language Models (LLM), Predictive AI, Natural Language Processing (NLP) และ Generative AI

(๒) งานด้านติดตามผลการดำเนินงานตามนโยบายรัฐบาลและข้อสั่งการนายกรัฐมนตรี โดยการนำ AI มาใช้ในการติดตามความคืบหน้าผลการดำเนินงานและข้อสั่งการ การแจ้งเตือนภารกิจสำคัญหรือหน่วยงานที่ดำเนินการล่าช้า การสรุปสถานะผลการดำเนินงาน การวิเคราะห์ความก้าวหน้า การวิเคราะห์ปัญหาและอุปสรรคในการดำเนินงาน และการจัดทำรายงานผู้บริหารแบบ Real-time เพื่อเพิ่มประสิทธิภาพในการติดตาม เร่งรัด วิเคราะห์ข้อมูล และรายงานผลการดำเนินงานได้อย่างเป็นระบบและทันเวลา เช่น Workflow AI, Reminder AI, Dashboard Analytics, Predictive AI, Robotic Process Automation (RPA), Intelligent Reporting, Natural Language Processing (NLP) และ Generative AI

(๓) งานด้านเอกสารราชการและงานสารบรรณ โดยการนำ AI มาใช้ในการร่างหนังสือราชการ สรุปสาระสำคัญของเอกสาร แปลงเอกสารเป็นข้อมูลดิจิทัล ตรวจสอบความถูกต้องของเอกสาร จัดหมวดหมู่เอกสาร และสืบค้นข้อมูล เพื่อช่วยลดระยะเวลาการดำเนินงาน เพิ่มความถูกต้องแม่นยำ และลดภาระงานประจำของบุคลากร รวมทั้งเพิ่มประสิทธิภาพในการจัดทำ ตรวจสอบ จัดเก็บ และค้นหาเอกสารราชการ ได้อย่างรวดเร็วและเป็นระบบ เช่น Generative AI, Natural Language Processing (NLP), Optical Character Recognition (OCR), Intelligent Document Processing (IDP), Speech-to-Text และ Document Analytics

(๔) งานประชุม โดยการนำ AI มาใช้สรุปรายงานการประชุม การถอดเสียงการประชุมเป็นข้อความ การจัดทำประเด็นสั่งการและสาระสำคัญจากการประชุม และการติดตามความคืบหน้ามติที่ประชุม รวมทั้งการแจ้งเตือนการดำเนินงานที่เกี่ยวข้องได้อย่างเป็นระบบ เพื่อเพิ่มประสิทธิภาพในการบันทึกสรุปและติดตามผลการประชุมได้อย่างรวดเร็วและแม่นยำ เช่น Speech-to-Text, AI Summarization, Task AI, Meeting Intelligence, Natural Language Processing (NLP) และ Generative AI

(๕) งานด้านสื่อสารและประชาสัมพันธ์ โดยการนำ AI มาใช้สรุปข่าวและประเด็นสำคัญ การวิเคราะห์แนวโน้มและกระแสสังคมออนไลน์ การจัดทำร่างข่าวประชาสัมพันธ์ การผลิตสื่อประชาสัมพันธ์ วิเคราะห์ความคิดเห็นของประชาชน การวางแผนการสื่อสารเชิงรุก และติดตามผลการเผยแพร่ข้อมูล เพื่อเพิ่มประสิทธิภาพในการผลิตสื่อ วิเคราะห์ความคิดเห็น และสื่อสารข้อมูลได้อย่างรวดเร็วและตรงกลุ่มเป้าหมาย เช่น Sentiment Analysis, Image AI, Social Media Analytics, Natural Language Processing (NLP), Text-to-Speech Recommendation AI, และ Generative AI

(๖) งานด้านบริหารบุคคลและพัฒนางานองค์กร โดยการนำ AI มาใช้วิเคราะห์ข้อมูลบุคลากร การประเมินสมรรถนะ สนับสนุนการวางแผนอัตรากำลังและพัฒนาศักยภาพบุคลากร การจัดทำข้อมูลประกอบการประเมินผล การวิเคราะห์แนวโน้มด้านบุคลากร ตลอดจนการสนับสนุนการพัฒนางานองค์กรและการจัดการองค์ความรู้ เพื่อเพิ่มประสิทธิภาพในการบริหารทรัพยากรบุคคล การพัฒนาศักยภาพบุคลากร และการวางแผนอัตรากำลังได้อย่างเป็นระบบ เช่น HR Analytics, Recommendation AI, Predictive AI, Talent Management AI, Chatbot AI และ Learning Analytics

(๗) งานด้านการพัฒนาระบบเทคโนโลยีสารสนเทศ โดยการนำ AI มาใช้สนับสนุนการพัฒนาโปรแกรมอัตโนมัติ ระบบงานภายใน ลดขั้นตอนการพัฒนา ทดสอบ และตรวจสอบประสิทธิภาพของระบบ การวิเคราะห์และคาดการณ์ปัญหาในระบบ การบริหารจัดการระบบสารสนเทศ รวมทั้งการตรวจจับและเฝ้าระวังเหตุผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเพิ่มประสิทธิภาพในการพัฒนา ดูแล และบริหารจัดการระบบสารสนเทศได้อย่างรวดเร็ว มีคุณภาพ และมีความมั่นคงปลอดภัย เช่น AI Coding Assistant, Low-Code & No-Code AI, Chatbot, Predictive Analytics, Test Automation, DevOps AI, Intelligent Monitoring และ Cybersecurity AI

(๘) งานด้านอื่น ๆ ที่สามารถใช้ปัญญาประดิษฐ์เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานได้

ทั้งนี้ การประยุกต์ใช้งาน AI ในแต่ละภารกิจ ต้องอยู่ภายใต้การกำกับดูแลและตรวจสอบ โดยผู้ใช้งานเป็นผู้รับผิดชอบผลลัพธ์ของการใช้งาน AI ในทุกกรณี

๕.๒ การบริหารจัดการข้อมูลเพื่อสนับสนุนการใช้งาน AI

ข้อมูลที่จะนำเข้าระบบ AI เพื่อให้วิเคราะห์ต่าง ๆ ต้องทำการเตรียมข้อมูล ตรวจสอบความถูกต้องของข้อมูล มีปริมาณมากเพียงพอ ไม่มีความลำเอียงหรือเลือกข้าง และเมื่อ AI วิเคราะห์แล้วต้องทำการตรวจสอบข้อมูล และดำเนินการตรวจสอบผลการวิเคราะห์หลาย ๆ รอบ ก่อนที่จะนำไปใช้งานจริง และต้องดำเนินการตามประกาศนโยบายและมาตรการการคุ้มครองข้อมูลส่วนบุคคลของสำนักเลขาธิการนายกรัฐมนตรี

๖. การกำกับดูแล

๖.๑ การกำกับดูแลตลอดวงจรชีวิตของ AI (AI Lifecycle Governance)

สำนักเลขาธิการนายกรัฐมนตรีกำหนดแนวทางการกำกับดูแลการใช้งาน AI ให้ครอบคลุมตลอดวงจรชีวิตของระบบ AI ดังนี้

(๑) การออกแบบโซลูชัน (Solution Design) ต้องกำหนดวัตถุประสงค์ ขอบเขต และผลลัพธ์ที่คาดหวังของการใช้ AI ให้สอดคล้องกับภารกิจของสำนักเลขาธิการนายกรัฐมนตรี พร้อมวิเคราะห์ความจำเป็นและความเหมาะสมก่อนนำ AI มาใช้ รวมทั้งเลือก AI ให้เหมาะสมกับลักษณะงาน งบประมาณ ความพร้อมของบุคลากร และความมั่นคงปลอดภัยของข้อมูล นอกจากนี้ ต้องกำหนดผู้รับผิดชอบโครงการ และผู้ดูแลระบบให้ชัดเจน มีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ตลอดจนกำหนดให้มีการกำกับดูแลโดยมนุษย์ (Human Oversight) สำหรับงานสำคัญก่อนนำผลลัพธ์ไปใช้งานจริง

(๒) การจัดเตรียมข้อมูล (Data Preparation) ต้องกำกับดูแลข้อมูลที่จะใช้กับ AI ให้มีความถูกต้อง ครบถ้วน ทันสมัย โดยใช้ข้อมูลที่มีการตรวจสอบคุณภาพข้อมูลก่อนนำไปใช้งาน รวมทั้งต้องกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคลของสำนักเลขาธิการนายกรัฐมนตรี เพื่อให้การใช้งาน AI มีประสิทธิภาพ โปร่งใส และสอดคล้องกับกฎหมาย และ นโยบายและมาตรการการคุ้มครองข้อมูลส่วนบุคคล ของสำนักเลขาธิการนายกรัฐมนตรี

(๓) การสร้างโมเดล (Model Development) ต้องพัฒนาหรือเลือก AI ให้เหมาะสมกับลักษณะงาน โดยคำนึงถึงความถูกต้อง ความน่าเชื่อถือ ความโปร่งใส ความมั่นคงปลอดภัย และความสามารถในการใช้งานจริง รวมถึงดำเนินการทดสอบความถูกต้อง อคติ ความมั่นคงปลอดภัย และการใช้งานจริงก่อนนำไปใช้งาน เพื่อให้มั่นใจว่า AI สามารถสนับสนุนภารกิจของสำนักเลขาธิการนายกรัฐมนตรีได้อย่างเหมาะสมและมีประสิทธิภาพ

(๔) การนำโมเดลไปใช้งาน (Deployment & Operation) ต้องมีการทดสอบการทำงานในสภาพแวดล้อมที่ใกล้เคียงการปฏิบัติงานจริง ประเมินความพร้อมของระบบ และบุคลากรก่อนเริ่มต้นใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้มีประสิทธิภาพและเชื่อมโยงกับระบบงานเดิมได้อย่างเหมาะสม ทั้งนี้ ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งมีแนวทางรองรับเหตุการณ์ผิดปกติหรือความคลาดเคลื่อนที่อาจเกิดขึ้น และกำหนดให้มีการกำกับดูแลโดยมนุษย์ (Human Oversight) ก่อนนำผลลัพธ์ไปใช้งานจริง

(๕) การติดตามการใช้งาน (Monitoring) ต้องติดตามและตรวจสอบประสิทธิภาพของการใช้งานความสำเร็จตามเป้าหมาย ความถูกต้องของผลลัพธ์ ข้อคิดเห็นและประเด็นปัญหาจากผู้ใช้งาน และการทบทวนและปรับปรุงระบบอย่างต่อเนื่อง

(๖) การประเมินผลการใช้งาน (Evaluation) ต้องประเมินผลสัมฤทธิ์ของการใช้ AI ในด้านการบรรลุเป้าหมายของโครงการ ประสิทธิภาพและความคุ้มค่าในการดำเนินงาน ความพึงพอใจของผู้ใช้งาน ความเสี่ยงและผลกระทบที่เกิดขึ้นจากการใช้งานจริง ความสอดคล้องกับกฎหมาย นโยบาย และจริยธรรม รวมทั้งจัดทำข้อเสนอเพื่อปรับปรุงหรือขยายผลการดำเนินงาน

(๗) การยุติการใช้งาน (Decommissioning) เมื่อ AI หมดความจำเป็น ไม่คุ้มค่าหรือล้าสมัย หรือมีความเสี่ยงสูง ต้องดำเนินการยุติการใช้งานโดยไม่ก่อให้เกิดความเสียหายต่อสำนักเลขาธิการนายกรัฐมนตรี รวมทั้งสื่อสารให้ผู้ใช้งานทราบ และรายงานผลต่อคณะกรรมการกำกับดูแลการใช้งาน AI

๖.๒ การบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI

เพื่อลดความเสี่ยงและผลกระทบจากการใช้งาน AI สำนักเลขาธิการนายกรัฐมนตรีได้กำหนดแนวทางการบริหารจัดการความเสี่ยง AI ในทุกกิจกรรมตลอดวงจรชีวิตให้อยู่ในระดับที่ยอมรับได้ โดยมีรายละเอียดดังนี้

(๑) การบริหารความเสี่ยงจากการใช้งาน AI

ประเภทความเสี่ยง	ประเด็นความเสี่ยง	การประเมินความเสี่ยง	มาตรการควบคุมความเสี่ยง
ด้านคุณภาพข้อมูล (Data Quality)	- ข้อมูลไม่ครบถ้วน - ข้อมูลไม่ถูกต้อง - ข้อมูลไม่เป็นปัจจุบัน - ข้อมูลคลาดเคลื่อน - ข้อมูลไม่มีแหล่งที่มาชัดเจน	- รายงานไม่ถูกต้อง - การตัดสินใจผิดพลาด - งานล่าช้า - ความน่าเชื่อถือลดลง	- ตรวจสอบแหล่งที่มาของข้อมูล - ปรับปรุงข้อมูลให้เป็นปัจจุบัน - ทบทวนผลลัพธ์โดยเจ้าหน้าที่ผู้รับผิดชอบ
ด้านความไม่เป็นธรรมและการเลือกปฏิบัติ (Unfairness and Discrimination)	- เรียนรู้ข้อมูลจากกลุ่มใดกลุ่มหนึ่งมากเกินไปทำให้การวิเคราะห์ข้อมูลเอนเอียง - ข้อมูลไม่ครบทุกกลุ่มทุกประเด็น	- เกิดความไม่เท่าเทียมในการพิจารณาเรื่องร้องเรียน - สร้างความเสียหายต่อความเชื่อมั่นของประชาชน - ขัดต่อหลักธรรมาภิบาล	- ใช้ข้อมูลที่หลากหลายและสมดุล - ทดสอบอคติของโมเดล - ให้นัผู้เชี่ยวชาญตรวจสอบก่อนตัดสินใจ
ด้านภัยคุกคามทางไซเบอร์ (Cyber Attack)	- การเข้าถึงระบบโดยไม่ได้รับอนุญาต - การโจมตีระบบ AI - การรั่วไหลของข้อมูลจากการนำไปใช้กับ AI - สาธารณะที่ไม่ปลอดภัย	- ข้อมูลราชการรั่วไหล - ระบบหยุดชะงัก - ระบบถูกโจมตีทางไซเบอร์ - กระทบต่อความมั่นคงปลอดภัยของหน่วยงาน	- กำหนดข้อจำกัดการใช้งานระบบภายนอก - เข้ารหัสข้อมูล - ควบคุมสิทธิการเข้าถึง - บันทึกและติดตามการใช้งาน
ด้านการคุ้มครองความเป็นส่วนตัว (Privacy)	- การใช้หรือเปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็นหรือใช้ผิดวัตถุประสงค์ - ใช้ข้อมูลส่วนบุคคลโดยไม่ปกปิด	- ละเมิดสิทธิส่วนบุคคล - เกิดข้อร้องเรียน - ถูกดำเนินคดี - เสียความเชื่อมั่น	- ปกปิดข้อมูลส่วนบุคคล - ใช้ข้อมูลเท่าที่จำเป็น - ตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
ด้านการไม่ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Non-Compliance)	- การใช้งานไม่สอดคล้องกับกฎหมาย ระเบียบราชการ นโยบายคุ้มครองข้อมูลส่วนบุคคล ลิขสิทธิ์ มาตรฐานความมั่นคงปลอดภัย - การสร้างสื่อประชาสัมพันธ์โดยใช้รูปภาพที่มีลิขสิทธิ์	- ถูกฟ้องร้องดำเนินคดี - ถูกตรวจสอบจากหน่วยงานที่เกี่ยวข้อง - เกิดความเสียหายทางราชการ	- ตรวจสอบด้านกฎหมายก่อนใช้งาน - กำหนดกระบวนการอนุมัติก่อนดำเนินการ - ใช้รายการตรวจสอบการปฏิบัติตามข้อกำหนด
ด้านความน่าเชื่อถือหรือชื่อเสียง (Trust and Reputation)	- สร้างข้อมูลผิดพลาดคลาดเคลื่อน - มีเนื้อหาที่ไม่เหมาะสม	- ประชาชนเข้าใจผิด - สูญเสียความเชื่อมั่นต่อหน่วยงาน - ส่งผลต่อภาพลักษณ์รัฐบาล	- ตรวจสอบความถูกต้องก่อนเผยแพร่ - กำหนดผู้มีอำนาจอนุมัติ

หมายเหตุ : ประเภทความเสี่ยง อ้างอิงตามแนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาลสำหรับผู้บริหารองค์กร โดยศูนย์ธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Clinic: AIGC) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

(๒) การบริหารจัดการความเสี่ยงตามวงจรชีวิต AI

ระยะวงจรชีวิต AI	ประเด็นความเสี่ยง	แนวทางควบคุมความเสี่ยง
การออกแบบโซลูชัน (Solution Design)	ใช้ AI ไม่ตรงวัตถุประสงค์	- จัดทำกรณีศึกษาความคุ้มค่า - กำหนดขอบเขตและวัตถุประสงค์โครงการ - อนุมัติโครงการตามลำดับชั้น - ประเมินความเสี่ยงเบื้องต้น
การจัดเตรียมข้อมูล (Data Preparation)	- ข้อมูลผิดพลาด - ข้อมูลรั่วไหล	- กำกับดูแลข้อมูล - ทำความสะอาดข้อมูล - จำแนกชั้นความลับข้อมูล - ปกปิดข้อมูลส่วนบุคคล - จำกัดสิทธิ์เข้าถึงข้อมูล
การสร้างโมเดล (Model Building)	- อคติของโมเดล - ความแม่นยำต่ำ	- ตรวจสอบความถูกต้องของโมเดล - ทดสอบประสิทธิภาพ - ทดสอบอคติของโมเดล - ทดสอบความมั่นคงปลอดภัย - ทบทวนผลลัพธ์โดยผู้เชี่ยวชาญ
การนำไปใช้งาน (Deployment)	- ใช้ผิดวัตถุประสงค์ - ผลลัพธ์ผิดพลาด	- จัดทำคู่มือการใช้งาน - ควบคุมสิทธิ์ผู้ใช้งาน - ให้นุชนตรวจสอบผลลัพธ์ก่อนใช้งาน - บันทึกการใช้งานระบบ - กำหนดผู้อนุมัติก่อนเผยแพร่
การติดตาม การใช้งาน (Monitoring)	- ประสิทธิภาพลดลง - ใช้งานไม่เหมาะสม	- ติดตามตัวชี้วัดผลการดำเนินงาน - รับข้อเสนอแนะจากผู้ใช้งาน - ตรวจสอบบันทึกการใช้งาน - ทบทวนฐานข้อมูลและคำสั่งใช้งาน
การประเมินผลการใช้งาน (Evaluation)	- ไม่คุ้มค่า - ไม่ตอบโจทย์ภารกิจ	- ประเมินผลตอบแทนจากการลงทุน - ประเมินความคุ้มค่าเชิงภารกิจ - ประเมินความเสี่ยงซ้ำ - สรุปรวความพึงพอใจผู้ใช้งาน
การยุติการใช้งาน (Retirement)	- ข้อมูลตกค้าง - ระบบเก่ายังถูกใช้งานต่อ	- จัดเก็บข้อมูลตามระยะเวลาที่กำหนด - ปิดสิทธิ์ผู้ใช้งาน - ถอนระบบอย่างเป็นทางการ - จัดทำแผนยุติการใช้งาน - สรุปรวทเรียนโครงการ

ทั้งนี้ ให้มีการจัดทำหรือทบทวนแผนบริหารความเสี่ยงให้เป็นปัจจุบัน และสอดคล้องกับสถานการณ์ ความเสี่ยง และเทคโนโลยีที่เปลี่ยนแปลงไปอย่างต่อเนื่อง โดยอาจพิจารณานำแนวทางมาตรฐาน ISO/IEC ๒๓๘๕๔:๒๐๒๓ Information technology - Artificial intelligence - Guidance on risk management มาใช้เป็นกรอบในการบริหารจัดการความเสี่ยง เพื่อให้การดำเนินการสอดคล้องกับมาตรฐานสากล

๗. ข้อควรปฏิบัติ (Do) และข้อห้ามปฏิบัติ (Don't)

๗.๑ ข้อควรปฏิบัติ (Do)

(๑) ต้องดำเนินการคัดกรองข้อมูลก่อนนำเข้าสู่ระบบ AI โดยพิจารณาใช้ข้อมูลเท่าที่จำเป็น (Data Minimization) และหลีกเลี่ยงการนำข้อมูลส่วนบุคคลหรือข้อมูลสำคัญของทางราชการเข้าสู่ระบบโดยไม่จำเป็น หรือหากจำเป็นควรใช้วิธีการปกปิดข้อมูล การทำข้อมูลนิรนาม (Anonymization) หรือการใช้นามแฝงข้อมูล (Pseudonymization) เมื่อสามารถดำเนินการได้ เพื่อป้องกันการเปิดเผยข้อมูลโดยไม่เหมาะสม

(๒) ต้องตรวจสอบความถูกต้อง ความครบถ้วน ความสมเหตุสมผล และความเหมาะสมของผลลัพธ์ที่ได้จาก AI ทุกครั้งก่อนนำไปใช้งาน เผยแพร่ หรือใช้ประกอบการตัดสินใจ โดยเฉพาะข้อมูลที่เกี่ยวข้องกับเอกสารราชการ ข้อมูลผู้บริหาร ข้อมูลเชิงนโยบาย หรือข้อมูลที่อาจส่งผลกระทบต่อสำนักเลขาธิการนายกรัฐมนตรีและประชาชน เพื่อป้องกันความคลาดเคลื่อน ข้อมูลเท็จ หรือการตีความที่ไม่ถูกต้อง

(๓) ต้องใช้ดุลพินิจของมนุษย์และเป็นผู้ตัดสินใจขั้นสุดท้าย (Human Judgment/Human Oversight) เพราะการใช้งาน AI เป็นเครื่องมือสนับสนุนการปฏิบัติงานเท่านั้น

(๔) ต้องระบุหรืออ้างอิงว่ามีการใช้ AI เป็นเครื่องมือสนับสนุน เมื่อมีการนำผลลัพธ์จาก AI ไปใช้จัดทำเอกสาร รายงาน สื่อประชาสัมพันธ์ หรือผลงานอื่นตามความเหมาะสมเพื่อให้เกิดความโปร่งใส และสามารถตรวจสอบได้

(๕) ต้องตรวจสอบเงื่อนไขการให้บริการ (Terms of Service) นโยบายความเป็นส่วนตัว (Privacy Policy) และมาตรการด้านความมั่นคงปลอดภัยของผู้ให้บริการ AI ภายนอกอย่างรอบคอบ ก่อนนำมาใช้งานกับข้อมูลของสำนักเลขาธิการนายกรัฐมนตรี

(๖) ต้องตรวจสอบความถูกต้อง ความปลอดภัย และช่องโหว่ของโค้ดที่ได้จาก AI ก่อนนำไปใช้งานจริง เพื่อป้องกันข้อผิดพลาดหรือความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี

(๗) ต้องใช้วิจารณญาณในการกำหนดคำสั่งหรือข้อความนำเข้า (Prompt) ให้เหมาะสม ชัดเจน และไม่ก่อให้เกิดอคติหรือผลลัพธ์ที่ไม่เหมาะสม รวมทั้งหลีกเลี่ยงการป้อนข้อมูลที่เป็นความลับหรือข้อมูลสำคัญของทางราชการเข้าสู่ระบบ AI โดยไม่จำเป็น

(๘) ต้องปฏิบัติตามกฎหมาย ระเบียบ มาตรการด้านความมั่นคงปลอดภัยสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี นโยบายและแนวทางปฏิบัติการใช้งานปัญญาประดิษฐ์ของสำนักเลขาธิการนายกรัฐมนตรี และแนวทางการคุ้มครองข้อมูลส่วนบุคคลของสำนักเลขาธิการนายกรัฐมนตรี

(๙) ต้องใช้ AI อย่างมีจริยธรรม เคารพสิทธิ เสรีภาพ ศักดิ์ศรีความเป็นมนุษย์ และไม่เลือกปฏิบัติ รวมทั้งต้องไม่นำ AI ไปใช้เพื่อสร้าง เผยแพร่ หรือสนับสนุนข้อมูลเท็จ ข้อมูลบิดเบือน หรือเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล หน่วยงาน หรือสังคม

(๑๐) ต้องรายงานต่อผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยทันที เมื่อพบเหตุผิดปกติ ความคลาดเคลื่อน หรือความเสี่ยงที่เกิดจากการใช้งาน AI เพื่อให้สามารถดำเนินการตรวจสอบ แก้ไข และควบคุมผลกระทบได้อย่างเหมาะสม

๗.๒ ข้อห้ามปฏิบัติ (Don't)

(๑) ห้ามป้อนข้อมูลภายในของสำนักเลขาธิการนายกรัฐมนตรีหรือข้อมูลที่เป็นความลับเข้าสู่ระบบ AI สาธารณะ เช่น รหัสผ่าน รายละเอียดการตั้งค่าระบบ (System Configuration) ใบรับรองดิจิทัล (Certificate) เอกสารลับ เอกสารสัญญา ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว รวมถึงข้อมูลในรูปแบบข้อความ ภาพ เสียง หรือวิดีโอที่สามารถระบุตัวบุคคลหรือสาระสำคัญของข้อมูลได้

(๒) ห้ามใช้ผลลัพธ์จาก AI โดยไม่ตรวจสอบข้อเท็จจริง แหล่งที่มา ความถูกต้อง ความครบถ้วน หรือความเหมาะสมก่อนนำไปใช้งาน อ้างอิง หรือเผยแพร่ในนามของสำนักเลขาธิการนายกรัฐมนตรี

(๓) ห้ามป้อนข้อมูลที่ไม่ได้รับการตรวจสอบความถูกต้อง หรือข้อมูลที่มีลักษณะบิดเบือน ซึ่งอาจส่งผลให้ AI ทำงานผิดพลาด (Data Poisoning)

(๔) ห้ามใช้ AI ในการตัดสินใจที่สำคัญ (High-Stakes Decisions) เช่น การพิจารณาอนุมัติ การลงโทษทางวินัย หรือการกำหนดนโยบาย โดยปราศจากการกลั่นกรอง การตรวจสอบ และการอนุมัติโดยมนุษย์ผู้มีอำนาจ เป็นต้น

(๕) ห้ามใช้ AI ในลักษณะที่ก่อให้เกิดอคติ การเลือกปฏิบัติ ความไม่เป็นธรรม หรือกระทบต่อสิทธิ เสรีภาพ และศักดิ์ศรีความเป็นมนุษย์

(๖) ห้ามใช้ AI เพื่อสร้าง เผยแพร่ หรือสนับสนุนข้อมูลเท็จ ข้อมูลบิดเบือน สื่อสังเคราะห์ปลอม หรือเนื้อหาที่อาจก่อให้เกิดความเข้าใจผิด กระทบต่อภาพลักษณ์ของสำนักเลขาธิการนายกรัฐมนตรี รัฐบาล ความมั่นคงของประเทศ หรือความสัมพันธ์ระหว่างประเทศ

(๗) ห้ามนำผลงานหรือผลลัพธ์ที่สร้างโดย AI ไปใช้แอบอ้างว่าเป็นผลงานของตนเอง ทั้งหมด โดยไม่เปิดเผยหรืออ้างอิงการใช้ AI ตามความเหมาะสม

(๘) ห้ามใช้ AI เพื่อสร้างหรือดัดแปลงเนื้อหาที่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น

(๙) ห้ามใช้ AI ในการจัดทำ วิเคราะห์ หรือเผยแพร่ข้อมูลเชิงนโยบาย ข้อมูลข่าวสารของสำนักเลขาธิการนายกรัฐมนตรี หรือข้อมูลที่มีผลกระทบต่อความเชื่อมั่นของประชาชน โดยไม่ได้รับการตรวจสอบและเห็นชอบจากผู้บริหารตามลำดับชั้น

(๑๐) ห้ามเชื่อมต่อ AI เข้ากับระบบสารสนเทศภายในของสำนักเลขาธิการนายกรัฐมนตรี โดยไม่ได้รับอนุญาต เช่น การเชื่อมต่อผ่าน API หรือการนำระบบไปฝังในระบบงาน (Integration) โดยไม่ได้ผ่านการประเมินความเสี่ยงและการอนุมัติจากผู้บังคับบัญชา

(๑๑) ห้ามใช้ AI ในทางที่ผิดกฎหมายและจริยธรรม (Misuse) รวมทั้งก่อให้เกิดภัยคุกคามทางไซเบอร์ เช่น การสร้างมัลแวร์ การโจมตีระบบ การสร้างสื่อปลอม (Deepfake) หรือการทำข้อความลวง (Phishing)

๘. การไม่ปฏิบัติตามนโยบาย

การไม่ปฏิบัติตามนโยบายฉบับนี้ หรือการดำเนินการใด ๆ ที่เป็นการหลีกเลี่ยงมาตรการควบคุม การกำกับดูแล หรือการตรวจสอบการใช้ AI ของสำนักเลขาธิการนายกรัฐมนตรี อาจมีผลให้ผู้กระทำผิด หรือผู้ฝ่าฝืนต้องรับผิดชอบของทางราชการ ข้อบังคับของสำนักเลขาธิการนายกรัฐมนตรี และกฎหมายที่เกี่ยวข้อง