

# อ่าน และ สรุปร Responsible Ai

Responsible AI เป็นแนวทางที่สำคัญในอุตสาหกรรมการเรียนรู้ของเครื่องในปัจจุบัน การผสานหลักการจริยธรรมในการพัฒนาโมเดลและการดำเนินงานขององค์กรไม่เพียงช่วยให้ผู้เชี่ยวชาญโดดเด่นและสร้างความไว้วางใจจากลูกค้า แต่ยังสร้างความได้เปรียบทางการแข่งขัน การทำ Responsible AI ไม่ควรถูกมองว่าแค่ทำตามข้อกำหนด แต่ต้องรวมถึงการพิจารณาอย่างรอบคอบว่าควรสร้างผลิตภัณฑ์หรือบริการนั้นหรือไม่

## 1. Fairness (ความเป็นธรรม)

ML ระบบต้องมีความเป็นธรรมสำหรับผู้ใช้งานทุกคน ไม่ควรมีความลำเอียง (bias) ต่อกลุ่มบุคคล เช่น เชื้อชาติ เพศ หรือสถานะทางเศรษฐกิจ เพื่อป้องกันไม่ให้โมเดลแสดงผลลัพธ์ที่อาจก่อให้เกิดการเลือกปฏิบัติ การวัดความเป็นธรรมสามารถใช้หลายวิธี เช่น การตรวจสอบการกระจายของผลลัพธ์และการพิจารณาว่ามีการตอบสนองต่อกลุ่มที่ต่างกันอย่างไร

## 2. Transparency (ความโปร่งใส)

การพัฒนา AI ที่รับผิดชอบจำเป็นต้องมีความโปร่งใสทั้งในกระบวนการพัฒนาและผลลัพธ์ ผู้ใช้งานควรทราบว่าโมเดลทำงานอย่างไร ใช้ข้อมูลประเภทใดบ้างในการฝึกสอน และการตัดสินใจของโมเดลมีที่มาจากอะไรบ้าง ควรมีเอกสารที่ชี้แจงรายละเอียดเกี่ยวกับวิธีการฝึกสอน โมเดล การประเมินผล และการเลือกตัวแปรต่างๆ ที่ใช้ในการพัฒนา

## 3. Explainability (การอธิบายได้)

ความสามารถในการอธิบายเหตุผลของผลลัพธ์ที่โมเดลให้มาเป็นสิ่งสำคัญ ผู้ใช้งานควรเข้าใจว่าโมเดลตัดสินใจอย่างไร เพื่อให้สามารถตรวจสอบได้หากเกิดข้อผิดพลาดหรือความไม่เป็นธรรม การทำให้โมเดลสามารถอธิบายได้ช่วยสร้างความไว้วางใจจากผู้ใช้งานและสังคม

## 4. Privacy (ความเป็นส่วนตัว)

การพัฒนา AI ต้องคำนึงถึงความเป็นส่วนตัวของข้อมูลผู้ใช้ เช่น การไม่ใช่ข้อมูลที่มีการระบุตัวตนได้ (personally identifiable information) และต้องมีการจัดการข้อมูลอย่างปลอดภัย แนวทางการปกป้องข้อมูลส่วนตัว เช่น differential privacy และการเข้ารหัสข้อมูล จะช่วยให้ข้อมูลถูกปกป้องในกระบวนการฝึกสอนและทำนาย

## 5. Security (ความปลอดภัย)

ระบบ AI ต้องได้รับการออกแบบให้มีความปลอดภัยต่อการโจมตีต่างๆ เช่น การโจมตีแบบ adversarial attack ซึ่งเป็นการป้อนข้อมูลที่ถูกรวบรวมมาเพื่อทำให้โมเดลทำงานผิดพลาด การทดสอบและสร้างระบบป้องกันการโจมตีเหล่านี้เป็นสิ่งสำคัญในการสร้าง AI ที่มีความปลอดภัย

## 6. Accountability (ความรับผิดชอบ)

ทีมพัฒนาต้องมีความรับผิดชอบต่อผลกระทบที่เกิดจากระบบ AI หากมีข้อผิดพลาดหรือผลลัพธ์ที่ก่อให้เกิดผลกระทบในทางลบ ต้องมีการรับผิดชอบและแก้ไขอย่างรวดเร็ว การกำหนดกรอบกฎหมายและนโยบายที่ชัดเจนสำหรับการใช้ AI ในบริบทต่างๆ จะช่วยให้เกิดความรับผิดชอบในการใช้งาน

หัวข้อนี้เป็นแนวทางสำคัญในการพัฒนา AI ที่ไม่เพียงแต่มีประสิทธิภาพ แต่ยังต้องมีความรับผิดชอบในด้านจริยธรรม ความเป็นธรรม และความปลอดภัย ซึ่งเป็นส่วนหนึ่งของการออกแบบระบบ Machine Learning ที่สามารถนำไปใช้งานในโลกความเป็นจริงได้อย่างยั่งยืน