ประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี
เรื่อง นโยบายและแนวปฏิบัติการใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์
(Artificial Intelligence: AI) เพื่อสนับสนุนพันธกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี
พ.ศ. ๒๕๖๙

.....

โดยที่เป็นการสมควรกำหนดนโยบายและแนวปฏิบัติการใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อสนับสนุนพันธกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี ให้สอดคล้องกับยุคแห่งการเปลี่ยนผ่านสู่สังคมดิจิทัล ปัญญาประดิษฐ์ ได้กลายเป็นเทคโนโลยีฐานรากที่มีบทบาทสำคัญต่อการขับเคลื่อนพันธกิจของสถาบันอุดมศึกษา ทั้งด้านการจัดการเรียนการสอน การบริหารจัดการ การวิจัย ปรับแปลงและถ่ายทอดเทคโนโลยี ตลอดจนการทำนุบำรุงศิลปวัฒนธรรม โดยมีโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์เป็นรากฐานสำคัญที่รองรับการพัฒนาและการให้บริการระบบปัญญาประดิษฐ์อย่างมีประสิทธิภาพ มั่นคง และปลอดภัย มหาวิทยาลัยเทคโนโลยีสุรนารี ตระหนักว่าการจัดหา พัฒนาและบริหารจัดการโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์จำเป็นต้องดำเนินการภายใต้หลักธรรมาภิบาล ความรับผิดชอบ ความโปร่งใส และการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อคงไว้ซึ่งความเป็นความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน ของระบบและข้อมูล ตลอดจนคุ้มครองสิทธิและความเป็นส่วนตัวของผู้เกี่ยวข้องทุกฝ่าย เพื่อให้การใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ (Artificial Intelligence: AI) สนับสนุนพันธกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี เป็นไปอย่างมีมาตรฐาน สอดคล้องกับกฎหมาย และมาตรฐานสากลที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๒๑ และมาตรา ๒๔ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. ๒๕๓๓ ประกอบกับคำสั่งสภามหาวิทยาลัยเทคโนโลยีสุรนารี ที่ ๔๐/๒๕๖๘ เรื่อง แต่งตั้งผู้รักษาการแทนอธิการบดี ลงวันที่ ๑๔ พฤศจิกายน ๒๕๖๘ คำสั่งสภามหาวิทยาลัยเทคโนโลยีสุรนารี ที่ ๑๗/๒๕๖๙ เรื่อง ขยายเวลาการรักษาการแทนอธิการบดี ลงวันที่ ๑๕ พฤษภาคม ๒๕๖๙ และมติที่ประชุมคณะกรรมการอำนวยการกำหนดนโยบายด้านปัญญาประดิษฐ์ในมหาวิทยาลัยเทคโนโลยีสุรนารี ในการประชุมครั้งที่ ๒/๒๕๖๙ เมื่อวันจันทร์ที่ ๒๒ มิถุนายน ๒๕๖๙ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี เรื่อง นโยบายและแนวปฏิบัติการใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพื่อสนับสนุนพันธกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย”	หมายความว่า	มหาวิทยาลัยเทคโนโลยีสุรนารี
“อธิการบดี”	หมายความว่า	อธิการบดีมหาวิทยาลัยเทคโนโลยีสุรนารี

“รองอธิการบดี”	หมายความว่า	รองอธิการบดีที่อธิการบดีมอบหมายให้กำกับดูแลหรือบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้บริหารระดับสูงด้านสารสนเทศ”	หมายความว่า	รองอธิการบดี ผู้กำกับดูแลและบริหารจัดการด้านระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศ”	หมายความว่า	รองอธิการบดี ผู้กำกับดูแลและบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ”	หมายความว่า	รองอธิการบดี ผู้รับผิดชอบการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ศูนย์คอมพิวเตอร์”	หมายความว่า	ศูนย์คอมพิวเตอร์มหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้อำนวยการ”	หมายความว่า	ผู้อำนวยการศูนย์คอมพิวเตอร์มหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้บังคับบัญชา”	หมายความว่า	ผู้ดำรงตำแหน่งบริหารสูงสุดของหน่วยงานที่บุคลากรผู้นั้นสังกัดอยู่
“ผู้ดูแลระบบ”	หมายความว่า	ผู้ซึ่งได้รับมอบหมายให้ปฏิบัติหน้าที่ดูแลระบบโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้ที่ได้รับมอบหมาย”	หมายความว่า	บุคคลหรือนิติบุคคลที่มหาวิทยาลัยมอบหมายให้ปฏิบัติงานตามภารกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ผู้ใช้งาน”	หมายความว่า	คณาจารย์ บุคลากร นักศึกษา และผู้ที่ได้รับมอบหมายให้ปฏิบัติงานตามภารกิจของมหาวิทยาลัยซึ่งใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ของมหาวิทยาลัยเทคโนโลยีสุรนารี
“คณาจารย์”	หมายความว่า	คณาจารย์มหาวิทยาลัยเทคโนโลยีสุรนารี

“บุคลากร”	หมายความว่า	พนักงาน ลูกจ้างของมหาวิทยาลัย หรือผู้ปฏิบัติงานในมหาวิทยาลัยที่มีชื่อเรียกเป็นอย่างอื่น ทั้งที่ปฏิบัติงานในสายวิชาการและสายสนับสนุนของมหาวิทยาลัยเทคโนโลยีสุรนารี
“นักศึกษา”	หมายความว่า	นักศึกษามหาวิทยาลัยเทคโนโลยีสุรนารี
“ปัญญาประดิษฐ์ หรือ (เอไอ/AI)”	หมายความว่า	ระบบหรือเทคโนโลยีสารสนเทศที่สามารถประมวลผล เรียนรู้ วิเคราะห์ หรือสร้างผลลัพธ์ในลักษณะที่จำลองความสามารถทางปัญญาของมนุษย์ ซึ่งนำมาใช้สนับสนุนการเรียนการสอน การประเมินผล หรือการบริหารจัดการทางวิชาการของมหาวิทยาลัยเทคโนโลยีสุรนารี
“เทคโนโลยี Generative AI”	หมายความว่า	เทคโนโลยีปัญญาประดิษฐ์ประเภทหนึ่งที่มีความสามารถในการสร้างเนื้อหาใหม่ได้หลากหลายรูปแบบตามข้อความหรือคำสั่ง ที่มนุษย์กำหนด เช่น ข้อความ ภาพ วิดีโอ ซอร์สโค้ด หรือเนื้อหาในรูปแบบอื่น
“วงจรชีวิตของปัญญาประดิษฐ์”	หมายความว่า	กระบวนการดำเนินงานของระบบปัญญาประดิษฐ์ตลอดช่วงอายุการใช้งาน ตั้งแต่ขั้นตอนการออกแบบและพัฒนา การนำไปใช้งานหรือให้บริการ ตลอดจนถึงการยุติการใช้งาน
“ข้อมูลส่วนบุคคล”	หมายความว่า	ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าโดยทางตรงหรือทางอ้อม ทั้งนี้ ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
“ข้อมูลส่วนบุคคลอ่อนไหว”	หมายความว่า	ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งมีลักษณะในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

ข้อ ๔ ขอบเขตการบังคับใช้

ประกาศนี้ให้ใช้บังคับกับการใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ทุกประเภทที่มหาวิทยาลัยจัดหา พัฒนา หรืออนุญาตให้นำมาใช้ เพื่อสนับสนุนการดำเนินงานตามพันธกิจของมหาวิทยาลัย ทั้งด้านการจัดการเรียนการสอน การบริหารจัดการ การวิจัย ปรับแปลงและถ่ายทอดเทคโนโลยี และการทำนุบำรุงศิลปวัฒนธรรม ทั้งนี้ ให้ครอบคลุมถึงคณาจารย์ บุคลากร นักศึกษา และผู้ที่ได้รับมอบหมายให้ปฏิบัติงานตามภารกิจของมหาวิทยาลัย

ข้อ ๕ หลักการทั่วไป

๕.๑ การบูรณาการปัญญาประดิษฐ์เข้ากับการดำเนินงานของมหาวิทยาลัยต้องดำเนินงานอย่างมีธรรมาภิบาล บนพื้นฐานของความเสมอภาคและเป็นธรรมโดยมหาวิทยาลัยให้ความสำคัญสูงสุดต่อการคุ้มครองความเป็นส่วนตัว สิทธิ เสรีภาพ และสิทธิมนุษยชนของผู้ใช้งานและผู้เกี่ยวข้องทุกฝ่าย ตลอดจนยึดมั่นในแนวปฏิบัติที่มนุษย์เป็นศูนย์กลางและมีอำนาจในการทบทวนและตัดสินใจขั้นสุดท้าย

๕.๒ การใช้โครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ต้องเป็นไปอย่างมีประสิทธิภาพและเกิดความคุ้มค่าเชิงทรัพยากร โดยมุ่งเป้าสู่วัตถุประสงค์เชิงยุทธศาสตร์ในการเพิ่มศักยภาพและยกระดับขีดความสามารถของนักศึกษาและบุคลากรของมหาวิทยาลัยเป็นสำคัญ

ข้อ ๖ ข้อห้ามและข้อจำกัดในการใช้งาน

ห้ามมิให้ผู้ใช้งานดำเนินการอย่างหนึ่งอย่างใด ดังต่อไปนี้

๖.๑ ใช้เป็นเครื่องมือชี้ขาดในการตัดสินใจที่มีนัยสำคัญหรือส่งผลกระทบสูงโดยปราศจากการทบทวน ตรวจสอบ และกำกับดูแลโดยมนุษย์ในขั้นตอนสุดท้าย

๖.๒ นำเข้าหรือป้อนข้อมูลที่ปราศจากการตรวจสอบความถูกต้องหรือมีเจตนาป้อนข้อมูลเพื่อบิดเบือนการประมวลผลและการเรียนรู้ของโมเดลปัญญาประดิษฐ์

๖.๓ ใช้ระบบเพื่อสนับสนุนพฤติการณ์อันเป็นภัยคุกคามทางไซเบอร์ในทุกรูปแบบ อาทิ การเขียนชุดคำสั่งประสงค์ร้าย การสร้างสื่อสังเคราะห์ปลอมเพื่อการหลอกลวง หรือการจำลอง ข้อความหลอกลวง ที่มีเจตนามุ่งร้าย

๖.๔ นำเข้าข้อมูลชั้นความลับของมหาวิทยาลัย ข้อมูลส่วนบุคคล หรือข้อมูลที่มีความละเอียดอ่อน เข้าสู่ระบบปัญญาประดิษฐ์โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรหรือขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๖.๕ ใช้ระบบเพื่อทำการละเมิดลิขสิทธิ์ ทรัพย์สินทางปัญญา หรือผลงานทางวิชาการของผู้อื่น

๖.๖ ใช้ระบบในกิจการที่ขัดต่อกฎหมาย ละเมิดศีลธรรมอันดีงามหรือการกระทำใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อบุคคล องค์กร และภาพลักษณ์ของมหาวิทยาลัยหรือสังคมโดยรวม

ข้อ ๗ แนวปฏิบัติด้านความซื่อสัตย์ทางวิชาการในการใช้เทคโนโลยี Generative AI

๗.๑ การกำหนดนโยบายระดับรายวิชา ให้คณาจารย์ผู้สอนมีอำนาจกำหนดขอบเขตการใช้งานเทคโนโลยี Generative AI ในรายวิชาของตน โดยต้องแจ้งให้นักศึกษาทราบอย่างชัดเจนในประมวลรายวิชาตั้งแต่ต้นภาคการศึกษา

๗.๒ การเปิดเผยการใช้งาน ในกรณีที่อนุญาตให้ใช้ Generative AI นักศึกษาต้องระบุอย่างชัดเจนว่าส่วนใดของงานที่ได้รับการสนับสนุนจาก AI รวมถึงระบุชื่อเครื่องมือ AI ที่ใช้ วันที่ใช้งาน และลักษณะของคำสั่งที่ใช้

๗.๓ การอ้างอิง ให้ถือว่าผลลัพธ์ที่ได้จากเทคโนโลยี Generative AI ไม่ใช่แหล่งข้อมูลปฐมภูมิ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องของข้อมูลและอ้างอิงแหล่งข้อมูลต้นฉบับเสมอ

๗.๔ ข้อห้ามในการสอบ ห้ามมิให้นักศึกษาใช้เทคโนโลยี Generative AI ในการทำข้อสอบหรือการประเมินผลที่กำหนดให้เป็นงานเฉพาะบุคคล เว้นแต่คณาจารย์ผู้สอนจะอนุญาตไว้เป็นลายลักษณ์อักษร

๗.๕ การส่งผลงานที่สร้างจาก AI ทั้งหมดโดยไม่เปิดเผย ให้ถือเป็นการกระทำทุจริตทางวิชาการ ซึ่งมหาวิทยาลัยจะดำเนินการตามกฎระเบียบหรือข้อบังคับของมหาวิทยาลัยว่าด้วยวินัยและบทลงโทษที่เกี่ยวข้อง

ข้อ ๘ ธรรมาภิบาลข้อมูลและความมั่นคงปลอดภัยของระบบ

เพื่อให้การบริหารจัดการระบบเป็นไปตามมาตรฐานสากล ให้หน่วยงานผู้รับผิดชอบพัฒนา หรือเป็นเจ้าของระบบปัญญาประดิษฐ์ ดำเนินการดังต่อไปนี้ อย่างเคร่งครัด

๘.๑ ออกแบบและพัฒนาโครงสร้างพื้นฐานดิจิทัลให้รองรับระบบปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย สอดคล้องกับระเบียบ ข้อบังคับ และมาตรฐานสากลที่เกี่ยวข้อง (อาทิ ISO/IEC 23894:2023 และ OWASP AI Exchange) โดยต้องบูรณาการมาตรการด้านความมั่นคงปลอดภัยเข้าไว้ในทุกระยะของวงจรการพัฒนาระบบ

๘.๒ กำหนดการตั้งค่าเริ่มต้นของระบบให้มีความมั่นคงปลอดภัยสูงสุดเพื่อจำกัดและลดพื้นที่การโจมตีทางไซเบอร์ ตลอดจนลดความเสี่ยงและบรรเทาผลกระทบที่อาจเกิดจากภัยคุกคาม

๘.๓ ตรวจสอบชุดคำสั่งหรือสคริปต์ที่สร้างหรือเกี่ยวข้องกับการใช้งานปัญญาประดิษฐ์อย่างละเอียด ก่อนนำไปเปิดใช้งานจริงเสมอ เพื่อค้นหาและอุดช่องโหว่หรือข้อผิดพลาดทางเทคนิค

๘.๔ มอบหมายหรือแต่งตั้งบุคลากรในสังกัดเพื่อทำหน้าที่เป็นผู้ดูแลระบบปัญญาประดิษฐ์ของหน่วยงาน พร้อมทั้งแจ้งบัญชีรายชื่อให้มหาวิทยาลัยทราบเป็นลายลักษณ์อักษร

๘.๕ บำรุงรักษา บริหารจัดการ และปรับปรุงระบบปัญญาประดิษฐ์อย่างสม่ำเสมอ เพื่อมิให้เกิดช่องโหว่หรือความเสี่ยงด้านความมั่นคงปลอดภัยรูปแบบใหม่

๘.๖ ยื่นความจำนงเพื่อขอเสนออนุมัติการเปิดให้บริการระบบปัญญาประดิษฐ์ต่อผู้บริหารระดับสูงด้านสารสนเทศของมหาวิทยาลัย ก่อนเปิดใช้งานอย่างเป็นทางการ

ข้อ ๙ การบริหารจัดการโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์

ให้ศูนย์คอมพิวเตอร์ ในฐานะหน่วยงานหลักผู้บริหารจัดการระบบโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ส่วนกลางของมหาวิทยาลัย มีหน้าที่รับผิดชอบและดำเนินการดังต่อไปนี้ อย่างเคร่งครัด

๙.๑ บริหารจัดการโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ของมหาวิทยาลัยให้สอดคล้องและเป็นไปตามกฎหมายที่เกี่ยวข้อง รวมถึงระเบียบและประกาศของมหาวิทยาลัย หรือที่แก้ไขเพิ่มเติม ดังนี้

๙.๑.๑ ระเบียบมหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วย การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๔

๙.๑.๒ ประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. ๒๕๕๔

๙.๑.๓ ประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๙.๒ กำหนดและบังคับใช้มาตรการควบคุมความมั่นคงปลอดภัยแบบหลายชั้น เพื่อให้ระบบโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ของมหาวิทยาลัย มีกลไกการป้องกันที่ครอบคลุมและส่งเสริมซึ่งกันและกันอย่างมีประสิทธิภาพ

๙.๓ จัดทำและทดสอบแผนการสำรองข้อมูลของระบบให้อยู่ในเกณฑ์มาตรฐานตามค่าเป้าหมายจุดฟื้นฟูข้อมูล หรือปริมาณข้อมูลที่ยอมรับให้สูญหายได้

๙.๔ จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ และแผนกู้คืนระบบสารสนเทศจากภัยพิบัติ พร้อมทั้งดำเนินการซักซ้อมเพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนด

๙.๕ เฝ้าระวังและติดตามการทำงานของระบบอย่างต่อเนื่อง หากตรวจพบความผิดปกติ พฤติกรรมที่น่าสงสัย หรือช่องโหว่ทางเทคนิค ให้ดำเนินการระงับเหตุเบื้องต้นและรายงานต่อผู้บังคับบัญชาหรือผู้บริหารที่เกี่ยวข้องรับทราบในทันที

๙.๖ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลการนำเข้า-นำออกของโมเดล และประวัติการบันทึกสิทธิ์ผู้ดูแลระบบ โดยต้องจัดเก็บรักษาไว้ไม่น้อยกว่าระยะเวลาที่กำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๙.๗ จัดทำข้อกำหนด เงื่อนไข และหลักเกณฑ์การขอใช้บริการช่องทางการเชื่อมต่อ เพื่อเป็นมาตรฐานกำกับการใช้งานสำหรับหน่วยงานอื่นภายในมหาวิทยาลัย

๙.๘ มอบหมายบุคลากรสังกัดศูนย์คอมพิวเตอร์ เพื่อปฏิบัติหน้าที่เป็นผู้ดูแลระบบและแจ้งบัญชีรายชื่อผู้รับผิดชอบให้มหาวิทยาลัยทราบเป็นลายลักษณ์อักษร

๙.๙ ให้คำปรึกษาและเสนอความเห็นทางเทคนิค ประกอบการพิจารณาของผู้บริหารระดับสูงด้านสารสนเทศ เพื่ออนุมัติการเปิดให้บริการระบบปัญญาประดิษฐ์ของหน่วยงานต่าง ๆ บนโครงสร้างพื้นฐานของมหาวิทยาลัย

๙.๑๐ เสนอขอความเห็นชอบต่อผู้บริหารระดับสูงด้านสารสนเทศ เพื่อใช้อำนาจสั่งการ “ระงับการให้บริการชั่วคราว” แก่ระบบปัญญาประดิษฐ์ที่ตรวจพบช่องโหว่ หรือมีความเสี่ยงด้านความมั่นคงปลอดภัยในระดับที่ต้องแก้ไขเร่งด่วน

๙.๑๑ เสนอขอความเห็นชอบต่อผู้บริหารระดับสูงด้านสารสนเทศ เพื่อใช้อำนาจสั่งการ “เพิกถอนและปิดการให้บริการถาวร” แก่ระบบปัญญาประดิษฐ์ที่มีช่องโหว่ ความเสี่ยงระดับร้ายแรง หรือขัดต่อหลักธรรมาภิบาลและข้อห้ามของมหาวิทยาลัยโดยไม่อาจแก้ไขได้

ข้อ ๑๐ การกำหนดสิทธิการเข้าถึงทรัพยากรและระบบสารสนเทศ

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเป็นไปอย่างมีประสิทธิภาพ ให้บุคลากรผู้ได้รับมอบหมายเป็นผู้ดูแลระบบปัญญาประดิษฐ์ประจำหน่วยงาน มีหน้าที่รับผิดชอบและดำเนินการ ดังต่อไปนี้ อย่างเคร่งครัด

๑๐.๑ กำหนดและบริหารจัดการสิทธิการเข้าถึงทรัพยากรและระบบปัญญาประดิษฐ์ให้มีความรัดกุม เหมาะสมกับภาระหน้าที่ และสอดคล้องกับระเบียบมหาวิทยาลัยเทคโนโลยีสุรนารีว่าด้วยการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๔

๑๐.๒ กำหนดให้ผู้เปิดใช้บริการ ต้องผ่านกระบวนการพิสูจน์และยืนยันตัวตนผ่านบัญชีผู้ใช้งานส่วนบุคคลของมหาวิทยาลัยก่อนเข้าใช้งานทุกครั้ง ทั้งนี้ ให้บังคับใช้การยืนยันตัวตนแบบหลายปัจจัย สำหรับบัญชีผู้ดูแลระบบที่มีสิทธิบริหารจัดการระบบปัญญาประดิษฐ์ของมหาวิทยาลัยอย่างเคร่งครัด

๑๐.๓ จัดทำตารางจำแนกและกำหนดสิทธิการเข้าถึงข้อมูลหรือทรัพยากร เพื่อใช้เป็นมาตรฐานในการควบคุมระดับสิทธิและการเข้าถึงระบบของผู้ใช้งานแต่ละกลุ่มอย่างชัดเจน

๑๐.๔ เฝ้าระวังและติดตาม การเข้าถึงระบบปัญญาประดิษฐ์อย่างต่อเนื่อง หากตรวจพบความผิดปกติ พฤติกรรมที่น่าสงสัย หรือการกระทำที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย ให้ดำเนินการตรวจสอบโดยพลัน และหากพบความเสี่ยง ให้ดำเนินการระงับสิทธิการใช้งานของผู้ใช้งานนั้น ในทันที พร้อมทั้งรายงานเหตุการณ์ต่อผู้บังคับบัญชาและหน่วยงานที่รับผิดชอบรับทราบโดยเร่งด่วน

ข้อ ๑๑ การรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล

เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลและปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้บุคลากรและผู้ใช้งานทุกคนยึดถือแนวปฏิบัติ ดังต่อไปนี้ อย่างเคร่งครัด

๑๑.๑ ห้ามมิให้ผู้ใดนำข้อมูลภายในของมหาวิทยาลัยหรือข้อมูลที่มีการจัดชั้นความลับ อาทิ รหัสผ่านระบบ เอกสารสัญญาที่มีผลผูกพันทางกฎหมาย ข้อมูลโครงการที่ยังไม่เปิดเผย หรือข้อมูลความลับทางการค้า นำเข้า ป้อน หรือประมวลผลร่วมกับระบบปัญญาประดิษฐ์ของมหาวิทยาลัย เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากมหาวิทยาลัย

๑๑.๒ ในกรณีที่มีความจำเป็นทางภาระงาน ที่ต้องใช้เทคโนโลยีปัญญาประดิษฐ์ในการประมวลผลข้อมูลภายในหรือข้อมูลส่วนบุคคล ให้จำกัดการใช้งานเฉพาะบน “ระบบปัญญาประดิษฐ์ที่มหาวิทยาลัยจัดเตรียมและรับรองกระบวนการแล้ว” เท่านั้น ห้ามมิให้นำไปประมวลผลบนระบบปัญญาประดิษฐ์สาธารณะภายนอกโดยเด็ดขาด ทั้งนี้ ผู้ใช้งานจะต้องเสนอขอรับการอนุมัติจากผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศก่อนเริ่มดำเนินการทุกครั้ง

ข้อ ๑๒ หลักการออกแบบที่มั่นคงปลอดภัย

ให้หน่วยงานผู้พัฒนาระบบ บูรณาการมาตรการบริหารจัดการความเสี่ยงในทุกระยะของวงจรการพัฒนาระบบเพื่อคาดการณ์ ป้องกัน และลดทอนความเสี่ยงที่อาจเกิดขึ้นกับสถาปัตยกรรมของระบบ โดยให้ยึดแนวทางปฏิบัติ ดังต่อไปนี้

๑๒.๑ การประเมินความเสี่ยง ดำเนินการประเมินความเสี่ยงและภัยคุกคามอย่างรอบด้าน เพื่อระบุช่องโหว่และความท้าทายที่เฉพาะเจาะจงของเทคโนโลยีปัญญาประดิษฐ์ ควบคู่ไปกับการประเมินภัยคุกคามที่อาจส่งผลกระทบต่อระบบโครงสร้างพื้นฐานดิจิทัลแบบดั้งเดิม

๑๒.๒ การลดหย่อนข้อมูลและการคุ้มครองความเป็นส่วนตัว ออกแบบระบบโดยยึดหลักการรวบรวมและจัดเก็บข้อมูลเท่าที่จำเป็น เพื่อลดพื้นที่เป้าหมายของการโจมตีทางไซเบอร์ ทั้งนี้ ให้ประยุกต์ใช้เทคโนโลยีกระดับความเป็นส่วนตัว อาทิ การทำข้อมูลให้เป็นนิรนาม หรือการใช้นามแฝง ตั้งแต่ขั้นตอนการออกแบบ ตลอดจนสร้างกลไกตรวจสอบความถูกต้องและแหล่งที่มาของข้อมูล เพื่อป้องกันความเสี่ยงจากการโจมตีด้วยการป้อนข้อมูลมุ่งร้าย

๑๒.๓ ความทนทานต่อการโจมตีเชิงปรปักษ์ คัดเลือกสถาปัตยกรรมโมเดลข้อมูลที่มีคุณสมบัติทนทานและพร้อมรับมือต่อการโจมตี พร้อมทั้งนำเทคนิคการฝึกสอนโมเดลเพื่อรับมือการหลอกลวง มาบูรณาการเป็นส่วนหนึ่งของกระบวนการพัฒนา เพื่อสร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยให้แก่ระบบตั้งแต่ต้นทาง

ข้อ ๑๓ หลักการตั้งค่าเริ่มต้นอย่างปลอดภัย

กำหนดให้การพัฒนาและบริหารจัดการระบบปัญญาประดิษฐ์ของมหาวิทยาลัยต้องบังคับใช้หลักการตั้งค่าเริ่มต้นอย่างปลอดภัย เพื่อยกระดับความมั่นคงปลอดภัยให้สูงสุด จำกัดและลดพื้นที่การโจมตีทางไซเบอร์ ตลอดจนบรรเทาผลกระทบจากภัยคุกคาม ทั้งนี้ ผู้รับผิดชอบระบบต้องดำเนินการตั้งค่าเริ่มต้นให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัย อย่างน้อยในประเด็น ดังต่อไปนี้

๑๓.๑ การควบคุมการเข้าถึง บังคับใช้หลักการให้สิทธิเท่าที่จำเป็น และหลักการความจำเป็นต้องรู้ โดยจำกัดและอนุญาตสิทธิเฉพาะบุคลากรที่ได้รับมอบหมาย ให้สามารถเข้าถึงและใช้งานข้อมูล ทรัพยากร หรือระบบปัญญาประดิษฐ์ได้เท่าที่จำเป็นแก่การปฏิบัติงานเท่านั้น

๑๓.๒ การพิสูจน์และยืนยันตัวตน กำหนดให้ต้องบังคับใช้การยืนยันตัวตนแบบหลายปัจจัยอย่างเคร่งครัด สำหรับบัญชีผู้ดูแลระบบที่มีสิทธิบริหารจัดการระบบปัญญาประดิษฐ์ เพื่อป้องกันความเสี่ยงจากการเข้าถึงระบบโดยมิชอบ หรือการโจรกรรมข้อมูลยืนยันตัวตน

๑๓.๓ การตรวจสอบและคัดกรองข้อมูลนำเข้า จัดให้มีกลไกตรวจสอบและคัดกรองข้อมูลก่อนนำเข้าสู่ระบบ เพื่อจำกัดรูปแบบและขอบเขตของข้อมูลให้อยู่ในสภาวะที่ปลอดภัย อันเป็นการป้องกันการโจมตีในรูปแบบการแทรกแซงฝังคำสั่งอันตราย และการบิดเบือนข้อมูล

๑๓.๔ ความมั่นคงปลอดภัยของส่วนต่อประสานในกระบวนการติดตั้งและกำหนดค่าเริ่มต้นของส่วนต่อประสานโปรแกรมประยุกต์ ต้องบังคับใช้กลไกการพิสูจน์และอนุญาตสิทธิอย่างเข้มงวด พร้อมทั้งเปิดใช้งานกลไกจำกัดอัตราการร้องขอ เพื่อป้องกันความเสี่ยงจากการโจมตีในรูปแบบการคัดลอกหรือขโมยปัญญาประดิษฐ์

๑๓.๕ การบันทึกข้อมูลและการเฝ้าระวัง จัดให้มีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลนำเข้า-นำออกของโมเดล และประวัติการใช้อำนาจของผู้ดูแลระบบอย่างครบถ้วน เพื่อใช้เป็นหลักฐานในการตรวจสอบร่องรอย การบุกรุก หรือการโจมตีไซเบอร์ที่อาจเกิดขึ้น อาทิ การลักลอบนำข้อมูลออก และการโจมตีเชิงปรปักษ์

ข้อ ๑๔ หลักการป้องกันเชิงลึก

กำหนดให้การพัฒนาและบริหารจัดการความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์ ต้องประยุกต์ใช้กลยุทธ์การป้องกันเชิงลึก ซึ่งเป็นมาตรการควบคุมและรักษาความมั่นคงปลอดภัยแบบยกระดับหลายชั้นที่ส่งเสริมซึ่งกันและกัน เพื่อชะลอ ยับยั้ง และจำกัดความเสียหายหากมาตรการชั้นใดชั้นหนึ่งถูกล่วงละเมิด โดยให้หน่วยงานที่เกี่ยวข้องบังคับใช้กลไกการควบคุมในแต่ละระดับของระบบ ดังต่อไปนี้

๑๔.๑ ระดับเครือข่าย ติดตั้งและใช้งานระบบไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน เพื่อคัดกรองและสกัดกั้นข้อมูลจราจรที่มุ่งร้ายต่อจุดเชื่อมต่อ พร้อมทั้งดำเนินการแบ่งย่อยส่วนเครือข่ายเพื่อบรรเทาและจำกัดขอบเขตความเสียหายหากเกิดการบุกรุก

๑๔.๒ ระดับแอปพลิเคชัน บังคับใช้นโยบายการพิสูจน์ยืนยันตัวตน และการอนุญาตสิทธิอย่างเข้มงวด ควบคู่กับการใช้กลไกตรวจสอบและคัดกรองข้อมูลเพื่อขจัดข้อมูลนำเข้าที่อาจเป็นอันตรายก่อนส่งไปยังโมเดลปัญญาประดิษฐ์ อันเป็นการป้องกันการโจมตีในรูปแบบการแทรกแซงฝังคำสั่ง

๑๔.๓ ระดับโมเดล เลือกใช้โมเดลปัญญาประดิษฐ์ที่ผ่านกระบวนการฝึกสอนเพื่อรับมือการโจมตีบูรณาการร่วมกับการติดตั้งกลไกตรวจสอบและกำกับผลลัพธ์เพื่อคัดกรองและสกัดกั้นการสร้างเนื้อหาที่ละเมิดข้อกำหนด ไม่เหมาะสม หรือเป็นอันตราย

๑๔.๔ ระดับข้อมูล บังคับใช้นโยบายการเข้ารหัสลับข้อมูล ทั้งข้อมูลที่อยู่ในสภาวะการจัดเก็บ และข้อมูลที่อยู่ระหว่างการส่งผ่าน ตลอดจนควบคุมสิทธิการเข้าถึงชุดข้อมูลสำหรับฝึกสอนโมเดล อย่างรัดกุมสูงสุด

๑๔.๕ ระดับปฏิบัติการและการเฝ้าระวัง จัดให้มีระบบบันทึกเหตุการณ์ และมาตรการเฝ้าระวังอย่างต่อเนื่อง เพื่อตรวจจับความผิดปกติ พฤติกรรมที่น่าสงสัย หรือความพยายามใด ๆ ที่อาจเป็นภัยคุกคามต่อระบบปัญญาประดิษฐ์ของมหาวิทยาลัย

ข้อ ๑๕ การจัดสรรงบประมาณเพื่อการพัฒนาและประยุกต์ใช้ปัญญาประดิษฐ์

๑๕.๑ ด้านโครงสร้างพื้นฐานระบบปัญญาประดิษฐ์

สนับสนุนงบประมาณสำหรับการจัดหา พัฒนา และยกระดับโครงสร้างพื้นฐานทางกายภาพ บริการระบบคลาวด์ ซอฟต์แวร์ ตลอดจนเครื่องมือและแพลตฟอร์มสำหรับการบริหารจัดการวงจรชีวิตของโมเดลปัญญาประดิษฐ์เชิงลึก (อาทิ MLOps Platform และ LLMOps Platform) ที่มีประสิทธิภาพสูง เพื่อผลักดันและสนับสนุนการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการขับเคลื่อนพันธกิจหลักขององค์กร ได้แก่ การจัดการเรียนการสอน การบริหารจัดการ การวิจัยปรับแปลง และถ่ายทอดเทคโนโลยี และการทำนุบำรุงศิลปวัฒนธรรม

๑๕.๒ ด้านโครงสร้างพื้นฐานและคลังข้อมูล

สนับสนุนงบประมาณสำหรับการพัฒนาและยกระดับเทคโนโลยีการจัดเก็บข้อมูลส่วนกลาง อาทิ ฐานข้อมูลเชิงสัมพันธ์ คลังข้อมูล และทะเลสาบข้อมูล เพื่อรองรับการไหลเวียน และประมวลผลข้อมูลขนาดใหญ่สำหรับการประยุกต์ใช้ปัญญาประดิษฐ์ในทุกพันธกิจและบริบทที่หลากหลายขององค์กร ตลอดจนสนับสนุนงบประมาณในการจัดทำมาตรฐานคำอธิบายชุดข้อมูลขององค์กรอย่างเป็นทางการ เพื่อยกระดับความก้าวหน้าด้านธรรมาภิบาลข้อมูล

ข้อ ๑๖ บทบาทหน้าที่และความรับผิดชอบ

๑๖.๑ ผู้บริหารระดับสูงด้านสารสนเทศ มีหน้าที่กำหนดวิสัยทัศน์ จัดทำนโยบายและแนวปฏิบัติ ตลอดจนกำกับดูแลภาพรวมการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในระดับยุทธศาสตร์ของมหาวิทยาลัย

๑๖.๒ ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่จัดทำนโยบาย กำหนดมาตรฐาน และกำกับดูแลกรอบการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศและการรับมือภัยคุกคาม สำหรับระบบปัญญาประดิษฐ์ของมหาวิทยาลัย

๑๖.๓ ผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่บริหารจัดการควบคุม และขับเคลื่อนมาตรการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับระบบปัญญาประดิษฐ์ให้เข้าสู่กระบวนการปฏิบัติงานจริงอย่างเป็นรูปธรรม

๑๖.๔ ศูนย์คอมพิวเตอร์ มีหน้าที่รับผิดชอบหลักในการจัดหา พัฒนา บำรุงรักษา และยกระดับระบบโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์ ส่วนกลางของมหาวิทยาลัย

๑๖.๕ ผู้ดูแลระบบโครงสร้างพื้นฐานดิจิทัล มีหน้าที่เฝ้าระวังและบริหารจัดการโครงสร้างพื้นฐานดิจิทัลด้านปัญญาประดิษฐ์อย่างต่อเนื่อง ตลอดจนมีหน้าที่ดำเนินการ “ระงับการให้บริการชั่วคราว” หรือ “เพิกถอนและปิดการให้บริการถาวร” แก่ระบบปัญญาประดิษฐ์ที่ตรวจพบช่องโหว่หรือความเสี่ยงด้านความมั่นคงปลอดภัยระดับร้ายแรง

๑๖.๖ หน่วยงานเจ้าของระบบ มีหน้าที่รับผิดชอบกระบวนการจัดหา พัฒนา และปรับปรุงระบบปัญญาประดิษฐ์ในสังกัดของหน่วยงานตนเอง อย่างต่อเนื่องตลอดวงจรชีวิตของการพัฒนาระบบ

๑๖.๗ ผู้ดูแลระบบปัญญาประดิษฐ์ประจำหน่วยงาน มีหน้าที่บริหารจัดการตั้งค่าสิทธิการเข้าถึง และเฝ้าระวังการทำงานของระบบปัญญาประดิษฐ์ที่อยู่ในความรับผิดชอบอย่างกวดขัน

๑๖.๘ ผู้ใช้งาน ต้องเป็นผู้รับผิดชอบต่อการตัดสินใจขั้นสุดท้าย ในกรณีที่มีการนำข้อมูล คำแนะนำ หรือผลลัพธ์จากระบบปัญญาประดิษฐ์ของมหาวิทยาลัยไปประยุกต์ใช้งาน โดยมีหน้าที่ตรวจสอบความถูกต้องของผลลัพธ์ก่อนนำไปเผยแพร่หรือใช้งานเสมอ ทั้งในด้านความถูกต้องแม่นยำ บริบทความเสมอภาคทางจริยธรรม และผลกระทบทางกฎหมาย ตลอดจนต้องรายงานต่อผู้บังคับบัญชาหรือผู้ดูแลระบบที่เกี่ยวข้องทราบในทันที หากตรวจพบว่าระบบปัญญาประดิษฐ์ประมวลผลผิดพลาด แสดงผลลัพธ์ที่มีอคติ หรือแสดงพฤติกรรมที่อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคลหรือมหาวิทยาลัย

ข้อ ๑๗ ให้คณะกรรมการดำเนินการประเมินและทบทวนความเหมาะสมของประกาศฉบับนี้อย่างน้อยทุก ๒ ปี หรือในกรณีที่มีพัฒนาการทางเทคโนโลยี การเปลี่ยนแปลงทางกฎหมาย หรือบริบทแวดล้อมอื่นใดที่ส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานของมหาวิทยาลัย ให้คณะกรรมการพิจารณาทบทวนและเสนอแนวทางการปรับปรุงต่อมหาวิทยาลัยเพื่อพิจารณาอนุมัติโดยเร็ว

ข้อ ๑๘ กรณีมีปัญหาจากการปฏิบัติตามประกาศนี้ ให้อธิการบดีเป็นผู้วินิจฉัยชี้ขาด คำวินิจฉัยของอธิการบดีให้ถือเป็นที่สุด

ประกาศ ณ วันที่ **๒๐ กรกฎาคม พ.ศ. ๒๕๖๙**

(รองศาสตราจารย์ ดร.สิทธิชัย แสงอาทิตย์)
รักษาการแทนอธิการบดีมหาวิทยาลัยเทคโนโลยีสุรนารี