คำสั่งมหาวิทยาลัยมหิดล
ที่ ๕๙๑/๒๕๖๙
เรื่อง แต่งตั้งผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
(Chief Information Security Officer: CISO)

เพื่อให้การบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยมหิดล สอดคล้องกับส่วนที่ ๓ สาระสำคัญข้อ ๓.๒.๑ การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐) ซึ่งกำหนดให้หน่วยงานจัดให้มีโครงสร้างการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศในระดับบริหารจัดการ ประกอบกับมหาวิทยาลัยมหิดลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ต้องจัดให้มีผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือเทียบเท่า เพื่อทำหน้าที่กำกับดูแล บริหารจัดการ และยกระดับขีดความสามารถในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการให้บริการสารสนเทศที่สำคัญของมหาวิทยาลัย

อาศัยอำนาจตามความในมาตรา ๓๔ (๑) และ (๘) แห่งพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ. ๒๕๕๐ ประกอบกับมติที่ประชุมคณะกรรมการบริหารมหาวิทยาลัยมหิดล ในการประชุมครั้งที่ ๒/๒๕๖๙ เมื่อวันที่ ๑๒ มกราคม พ.ศ. ๒๕๖๙ อธิการบดีมหาวิทยาลัยมหิดลจึงแต่งตั้ง ดร.ภทรภรต ภภัทร์สทธรรม ที่ปรึกษามหาวิทยาลัยด้านสารสนเทศและดิจิทัลทรานส์ฟอร์เมชัน เป็นผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) โดยให้มีอำนาจหน้าที่ ดังนี้

๑. ด้านนโยบายและแผน: กำหนดทิศทาง จัดทำ และปรับปรุงนโยบาย แนวปฏิบัติ และมาตรฐานในการรักษาความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย ให้สอดคล้องกับกฎหมาย มาตรฐานสากล และประกาศของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. ด้านการบริหารจัดการความเสี่ยง: กำกับดูแลให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ พร้อมทั้งเสนอแนะมาตรการในการป้องกันและลดความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศและการให้บริการของมหาวิทยาลัย

๓. ด้านการกำกับดูแลและติดตาม: ตรวจสอบและควบคุมดูแลการดำเนินงานของส่วนงานต่าง ๆ ภายในมหาวิทยาลัย ให้เป็นไปตามนโยบายและมาตรฐานที่กำหนด รวมถึงกำกับดูแลให้มีการตรวจสอบความปลอดภัย (Security Audit) ตามวงรอบที่เหมาะสม

๔. ด้านการตอบโต้ภัยคุกคาม: อำนวยการและตัดสินใจในกระบวนการตอบโต้สถานการณ์ฉุกเฉิน หรือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับมหาวิทยาลัย รวมถึงการจัดตั้งหรือบริหารจัดการทีมตอบโต้เหตุการณ์ความไม่ปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) ของมหาวิทยาลัย

๕. ด้านการประสานงานและรายงาน: ทำหน้าที่เป็นตัวแทนหลักของมหาวิทยาลัยในการประสานงานกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานควบคุมหรือกำกับดูแล (Regulator) และหน่วยงานภายนอกที่เกี่ยวข้อง พร้อมทั้งรายงานสถานะความมั่นคงปลอดภัยไซเบอร์ต่ออธิการบดีหรือคณะกรรมการที่เกี่ยวข้องอย่างสม่ำเสมอ

๖. ด้านการสร้างความตระหนักรู้: ส่งเสริมและสนับสนุนให้มีการฝึกอบรม พัฒนาทักษะ และสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้บริหาร บุคลากร และนักศึกษา เพื่อลดความเสี่ยงที่เกิดจากปัจจัยด้านบุคคล

๗. ด้านการพัฒนาและนวัตกรรม: เสนอแนะแนวทางในการจัดสรรงบประมาณและทรัพยากรเพื่อการพัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศให้มีความทันสมัยและมีประสิทธิภาพ

๘. ด้านการบริหารการเปลี่ยนแปลง: กำกับดูแลการเตรียมความพร้อมของระบบสารสนเทศและนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อรองรับการเปลี่ยนแปลงทางเทคโนโลยีขั้นสูง รวมถึงผลกระทบจากเทคโนโลยีควอนตัมในอนาคต

๙. ปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมายจากอธิการบดี เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๗ กุมภาพันธ์ พ.ศ.๒๕๖๙

(ศาสตราจารย์ นายแพทย์ปิยะมิตร ศรีธรา)
อธิการบดีมหาวิทยาลัยมหิดล