ตรวจสอบสำเนา+ARC

เลขที่รับ 2769
วันที่ 28 มี.ค. 2569
เวลา 10.50

ประกาศมหาวิทยาลัยมหิดล

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Policy)

พ.ศ. ๒๕๖๙

.....

เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการบริการสำคัญของมหาวิทยาลัยมหิดล มีความมั่นคงปลอดภัยไซเบอร์ สอดคล้องตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และเป็นไปตามนโยบาย แนวปฏิบัติ และมาตรฐานสากลที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศและทางไซเบอร์ อันเป็นการสร้างความเชื่อมั่นในการดำเนินภารกิจของมหาวิทยาลัย

อาศัยอำนาจตามความในมาตรา ๓๔ (๘) แห่งพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ. ๒๕๕๐ และมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการบริหารมหาวิทยาลัยมหิดล ครั้งที่ ๕/๒๕๖๙ เมื่อวันที่ ๒ กุมภาพันธ์ พ.ศ. ๒๕๖๙ อธิการบดีจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Policy) ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“คณะกรรมการบริหารมหาวิทยาลัย” หมายความว่า ที่ประชุมของผู้บริหารมหาวิทยาลัย ซึ่งประกอบด้วยอธิการบดีเป็นประธาน รองอธิการบดี ผู้ช่วยอธิการบดี และบุคคลอื่นตามที่อธิการบดีเห็นสมควรเป็นกรรมการ เพื่อบริหารงานของมหาวิทยาลัย

“ส่วนงาน” หมายความว่า สำนักงานสภามหาวิทยาลัย สำนักงานอธิการบดี คณะ และส่วนงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะ

“หน่วยงาน” หมายความว่า หน่วยงานภายในส่วนงาน

หมวด ๑
การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์
(Good Governance in Cybersecurity)

ข้อ ๒ การจัดโครงสร้างองค์กรและการถ่วงดุลอำนาจ

(๑) มหาวิทยาลัยต้องจัดให้มีโครงสร้างองค์กรที่เอื้อต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ไว้อย่างชัดเจน มุ่งเน้นการถ่วงดุลอำนาจตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ ดังนี้

ระดับที่ ๑ ส่วนงาน หน่วยงาน และผู้ปฏิบัติงาน (First Line of Defense) ส่วนงานหรือหน่วยงานที่เป็นเจ้าของระบบสารสนเทศ มีหน้าที่ดูแลและปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ที่มหาวิทยาลัยกำหนด พร้อมจัดให้มีการควบคุมภายในและการจัดการความเสี่ยงในระดับส่วนงานหรือหน่วยงาน แล้วแต่กรณีอย่างเหมาะสม

ระดับที่ ๒ หน่วยงานกำกับดูแล (Second Line of Defense) หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง (Risk Management) และหรือกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) ของมหาวิทยาลัย มีหน้าที่สนับสนุน กำหนดมาตรฐาน และติดตามการปฏิบัติงานของส่วนงานให้เป็นไปตามนโยบาย

ระดับที่ ๓ หน่วยงานตรวจสอบ (Third Line of Defense) หน่วยงานที่ทำหน้าที่ตรวจสอบภายใน (Internal Audit) ของมหาวิทยาลัย มีหน้าที่ตรวจสอบและประเมินผลอย่างเป็นอิสระ เพื่อให้เกิดกลไกการตรวจสอบและถ่วงดุลที่เป็นธรรมและมีประสิทธิผล

(๒) กรณีที่ส่วนงานหรือหน่วยงานมีการใช้ระบบสารสนเทศ หรือบริการเทคโนโลยีสารสนเทศร่วมกันหรือเป็นการใช้บริการผ่านระบบกลางของมหาวิทยาลัย การจัดโครงสร้างการกำกับดูแลตาม (๑) ให้พิจารณาจากภาพรวมของระบบนิเวศด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยเป็นสำคัญ เพื่อลดความซ้ำซ้อนในการดำเนินงานและเพื่อให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ครอบคลุมทุกมิติของมหาวิทยาลัย

ข้อ ๓ การกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(๑) มหาวิทยาลัยต้องจัดให้มีผู้ดำรงตำแหน่งประเภทผู้บริหารหรือผู้ที่อธิการบดีมอบหมาย เป็นผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย (Head of Information Security) เพื่อรับผิดชอบการกำหนดนโยบายและกำกับดูแลภาพรวมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย โดยต้องเป็นผู้ที่มีความรู้ ความเชี่ยวชาญ หรือมีประสบการณ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management) รวมถึงมีทักษะในการประเมินและรับมือกับภัยคุกคามทางไซเบอร์ เพื่อให้สามารถสนับสนุนการดำเนินภารกิจของมหาวิทยาลัยให้เป็นไปอย่างต่อเนื่องและปลอดภัย

(๒) การปฏิบัติหน้าที่ของผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย ให้พิจารณาจัดลำดับสายการรายงานหรือโครงสร้างอำนาจหน้าที่ที่มีความเป็นอิสระจากการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) โดยตรง เพื่อให้เกิดการตรวจสอบและถ่วงดุลตามหลักการกำกับดูแลที่ดี (Good Governance) โดยมีบทบาทหน้าที่และความรับผิดชอบอย่างน้อย ดังต่อไปนี้

(๒.๑) การกำหนดมาตรฐาน กำหนดนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย ให้สอดคล้องกับกฎหมายและมาตรฐานสากล รวมถึงกำกับดูแลให้ส่วนงานและหน่วยงานมีการปฏิบัติตามอย่างเคร่งครัด

(๒.๒) การวางโครงสร้างระบบ กำหนดข้อกำหนดด้านความมั่นคงปลอดภัย (Security Specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT Security Architecture) ของมหาวิทยาลัย เพื่อใช้เป็นมาตรฐานกลางในการจัดหาหรือพัฒนาระบบสารสนเทศ

(๒.๓) การบริหารความเสี่ยง บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ ให้สอดคล้องกับระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ (Risk Appetite) และนำเสนอรายงานสถานะความเสี่ยงต่อคณะกรรมการบริหารมหาวิทยาลัย หรือคณะกรรมการที่เกี่ยวข้องเป็นวาระประจำ

(๒.๔) การเตรียมความพร้อม กำกับดูแลและดำเนินการให้มหาวิทยาลัยมีความพร้อมในการรับมือและฟื้นฟูระบบจากภัยคุกคามทางไซเบอร์ (Cyber Resilience) เพื่อลดผลกระทบต่อภารกิจด้านการศึกษา การวิจัย และการบริการ

(๒.๕) การสร้างความตระหนักรู้ ส่งเสริมและดำเนินการให้บุคลากรและนักศึกษามีความรู้และความตระหนักรู้เกี่ยวกับความเสี่ยง รวมถึงแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างวัฒนธรรมความปลอดภัยทางดิจิทัลภายในมหาวิทยาลัย

(๓) ส่วนงานหรือหน่วยงานอาจพิจารณามอบหมายผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศภายในส่วนงานหรือหน่วยงาน เพื่อประสานงานและขับเคลื่อนการดำเนินงานให้สอดคล้องกับมาตรฐานที่มหาวิทยาลัยกำหนด

ข้อ ๔ การกำหนดให้มีผู้บริหารระดับสูงทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(๑) มหาวิทยาลัยต้องจัดให้มีผู้ดำรงตำแหน่งประเภทบริหารระดับกลาง หรือผู้ที่อธิการบดีมอบหมายเป็นผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย (Chief Information Security Officer: CISO) โดยต้องเป็นผู้ที่มีความเป็นอิสระจากงานด้านปฏิบัติการเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านการพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) รวมทั้งมีอำนาจหน้าที่ (Authority) เพียงพอในการกำกับดูแลและสั่งการ เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

(๒) การปฏิบัติหน้าที่ของผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยมีบทบาทหน้าที่และความรับผิดชอบอย่างน้อย ดังต่อไปนี้

(๒.๑) การรายงานอุบัติการณ์สำคัญ รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามที่เกิดขึ้นต่ออธิการบดี คณะกรรมการบริหารมหาวิทยาลัย หรือคณะกรรมการอื่นที่เกี่ยวข้อง แล้วแต่กรณี เพื่อให้เกิดการตัดสินใจและแก้ไขปัญหาได้อย่างทันท่วงที

(๒.๒) การเสนอความเห็นและร่วมตัดสินใจ ให้ความเห็นเชิงกลยุทธ์ด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงต่อคณะกรรมการบริหารมหาวิทยาลัย หรือคณะกรรมการอื่นที่เกี่ยวข้อง เช่น คณะกรรมการที่กำกับดูแลด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย และคณะกรรมการบริหารความเสี่ยง เป็นต้น โดยร่วมตัดสินใจในมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบต่อภารกิจหลักหรือชื่อเสียงของมหาวิทยาลัยอย่างมีนัยสำคัญ

หมวด ๒
การบริหารความเสี่ยง (Risk Management)

ข้อ ๕ การจัดทำกรอบการบริหารความเสี่ยง มหาวิทยาลัยและส่วนงานต้องจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร เพื่อให้การจัดการความเสี่ยงสอดคล้องกับบริบทตามพันธกิจของมหาวิทยาลัย โดยกรอบดังกล่าวต้องครอบคลุมเนื้อหา ดังนี้

(๑) การระบุเกณฑ์การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการกำหนดระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ (Risk Appetite) เพื่อเป็นเกณฑ์ในการตัดสินใจดำเนินการจัดการความเสี่ยง

(๒) วิธีการและขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับสินทรัพย์สารสนเทศของมหาวิทยาลัย

(๓) กระบวนการเฝ้าระวังและติดตามความเปลี่ยนแปลงของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

ข้อ ๖ ทะเบียนความเสี่ยง (Risk Register) มหาวิทยาลัยและส่วนงานต้องจัดทำและเก็บรักษารายการความเสี่ยงไว้ใน “ทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Register)” โดยเฉพาะความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศหรือบริการที่สำคัญของมหาวิทยาลัย เช่น ระบบฐานข้อมูลนักศึกษา ระบบฐานข้อมูลบุคลากร ระบบฐานข้อมูลผู้รับบริการทางการแพทย์ ระบบสารสนเทศทางการแพทย์ และระบบการเงินและพัสดุ เป็นต้น

ข้อ ๗ การติดตามความเสี่ยง มหาวิทยาลัยและส่วนงานต้องมีการติดตามความเสี่ยงที่ระบุไว้อย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามาตรการควบคุมที่มีอยู่สามารถรักษาความเสี่ยงให้อยู่ภายใต้ระดับที่มหาวิทยาลัยยอมรับได้ (Risk Appetite) ตามข้อ ๕ (๑)

ทั้งนี้ มหาวิทยาลัยต้องจัดให้มีการตรวจสอบและทบทวนมาตรการที่ใช้ในการควบคุมการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อยืนยันว่ามาตรการที่เคยกำหนดไว้ยังคงมีประสิทธิภาพและเพียงพอต่อภัยคุกคามรูปแบบใหม่ที่เกิดขึ้น

หมวด ๓
นโยบายและแนวปฏิบัติ (Policies and Guidelines)

ข้อ ๘ การกำหนดและประกาศใช้นโยบาย มหาวิทยาลัยต้องจัดให้มีการกำหนดและอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงและการป้องกันระบบสารสนเทศสำคัญของมหาวิทยาลัยจากภัยคุกคามทางไซเบอร์ โดยนโยบายและแนวปฏิบัติดังกล่าวต้อง

(๑) สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และมาตรฐานสากลที่เกี่ยวข้อง รวมถึงพิจารณาถึงความสอดคล้องตามบริบทการดำเนินงานของมหาวิทยาลัย

(๒) เผยแพร่และสื่อสารไปยังบุคลากร นักศึกษา และบุคคลภายนอก เช่น คู่ค้าหรือผู้ให้บริการภายนอก เป็นต้น ที่สามารถเข้าถึงหรือใช้งานระบบสารสนเทศของมหาวิทยาลัย เพื่อให้ทราบและถือปฏิบัติอย่างเคร่งครัด

ข้อ ๙ การทบทวนนโยบาย มหาวิทยาลัยต้องดำเนินการทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติให้สอดคล้องกับสภาพแวดล้อมทางเทคโนโลยีและภูมิทัศน์ของภัยคุกคามไซเบอร์ (Threat Landscape) ที่เปลี่ยนแปลงไป อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระบบสารสนเทศของมหาวิทยาลัย

บทเฉพาะกาล

ข้อ ๑๐ ให้ผู้ได้รับแต่งตั้งเป็นผู้บริหารระดับสูงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่ในวันที่ประกาศนี้มีผลใช้บังคับ เป็นผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยตามประกาศนี้ และให้ปฏิบัติหน้าที่ต่อไปจนกว่าจะมีผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยตามประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

งานเทคโนโลยีสารสนเทศ
รับที่ 28 เม.ย. 69
13.00 น.

ประกาศ ณ วันที่ ๒๗ เมษายน พ.ศ.๒๕๖๙

เรียน คณบดี ผ่านรองคณบดีฝ่ายบัณฑิตศึกษา
- เพื่อโปรดทราบ
- เห็นควรแจ้งทุกส่วนงาน

5 พ.ค. 69

(ศาสตราจารย์ นายแพทย์ปิยะมิตร ศรีธรา)
อธิการบดีมหาวิทยาลัยมหิดล

เรียน คณบดี
เพื่อโปรดทราบ
ทีม มว. IT เสนอครับ
11 พ.ค. 69

☑ ทราบ
☐ ทราบและดำเนินการได้
☐ อนุมัติ ☐ ไม่อนุมัติ
☐ อนุญาต
ลงนาม..........
11 พ.ค. 69

(รองศาสตราจารย์ เภสัชกรสุรกิจ นาฑีสุวรรณ)
คณบดีคณะเภสัชศาสตร์