ประกาศ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล

เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ นั้น

เพื่อให้การดำเนินการใด ๆ ด้านเทคโนโลยีสารสนเทศของ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และมีการพัฒนาปรับปรุงความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล จึงเห็นควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “นโยบายความมั่นคงปลอดภัยสารสนเทศ”

ข้อ ๒ นโยบายความมั่นคงปลอดภัยสารสนเทศ กำหนดให้มีสาระสำคัญเพื่อการนำไปดำเนินงานด้านความมั่นคงปลอดภัยในกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ดังนี้

ข้อ ๒.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ

ข้อ ๒.๑.๑ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง

ข้อ ๒.๑.๒ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องควบคุมให้มีการกำหนดสิทธิการใช้งานของผู้ใช้งานตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย รวมถึงการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

ข้อ ๒.๑.๓ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องดำเนินการฝึกอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศอย่าสม่ำเสมอ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากร

ข้อ ๒.๑.๔ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

... / ข้อ ๒.๑.๕

ข้อ ๒.๑.๕ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องควบคุมการเข้าถึงระบบปฏิบัติการเพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

ข้อ ๒.๑.๖ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๒.๒ การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

ข้อ ๒.๓ การตรวจสอบและประเมินความเสี่ยง

กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อให้กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๓ การจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล

กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ต้องจัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศนโยบายและแนวปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติได้ และต้องกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

ข้อ ๔ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้รองอธิการบดีที่กำกับดูแลกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๕ กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล กำหนดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑ ข้อ ได้แก่

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๓. การบริหารจัดการสินทรัพย์สารสนเทศ

๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

... / ๕.

๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ ๖ ให้มีการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ ให้บุคลากรของกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ได้มีประกาศไว้

ข้อ ๘ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑๕ พฤศจิกายน พ.ศ.๒๕๖๕

(ผู้ช่วยศาสตราจารย์ ดร.ธัชวีร์ ลีละวัฒน์)

รองอธิการบดีฝ่ายสารสนเทศและวิทยาเขตกาญจนบุรี