ประกาศมหาวิทยาลัยแม่โจ้
เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยแม่โจ้

เพื่ออนุวัติการให้เป็นไปตามความในมาตรา ๕ และมาตรา ๗ ภายใต้พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งกำหนดให้ “หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ที่กำหนดให้ “หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร จึงเป็นการสมควรกำหนดแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยแม่โจ้ โดยมีวัตถุประสงค์ ๑) เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของมหาวิทยาลัยแม่โจ้ ให้สามารถดำเนินไปได้อย่างมีประสิทธิภาพ ๒) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ อ้างอิงตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) และมีการปรับปรุงอย่างต่อเนื่อง และ ๓) เพื่อเผยแพร่และส่งเสริมให้เจ้าหน้าที่ผู้ดูแลระบบ ผู้ใช้งานระบบ และผู้ที่เกี่ยวข้อง มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และถือปฏิบัติตามอย่างเคร่งครัด ตามหลักจริยธรรมและหลักกฎหมาย

อาศัยอำนาจตามความในมาตรา ๓๒ และมาตรา ๓๘ (๑) แห่งพระราชบัญญัติมหาวิทยาลัยแม่โจ้ พ.ศ. ๒๕๖๐ ประกอบกับมติที่ประชุมคณะกรรมการบริหารมหาวิทยาลัย ในการประชุมครั้งที่ ๑๕/๒๕๖๓ เมื่อวันที่ ๑๗ สิงหาคม พ.ศ. ๒๕๖๓ จึงกำหนดแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยแม่โจ้ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยแม่โจ้”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศมหาวิทยาลัยแม่โจ้ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ฉบับลงวันที่ ๕ ตุลาคม พ.ศ. ๒๕๖๑

ข้อ ๔ ให้มหาวิทยาลัยจัดทำแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ โดยกำหนดให้มีสาระสำคัญสองส่วน ดังนี้

๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) กำหนดให้มีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลาหนึ่งครั้งต่อปี

๔.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย ประกอบด้วย ๓ ส่วน คือ

ส่วนที่ ๑ คำนิยาม

ส่วนที่ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ซึ่งกำหนดผู้รับผิดชอบตามนโยบาย มีสาระสำคัญสอดคล้องตามมาตรา ๕ และมาตรา ๗ ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ ดังนี้

(๑) นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

กำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้

กำหนดผู้รับผิดชอบนโยบาย ดังนี้

๑) ผู้อำนวยการกองเทคโนโลยีดิจิทัล

๒) รองอธิการบดีผู้รับผิดชอบดูแลกองเทคโนโลยีดิจิทัล

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๔) ผู้ใช้งาน

โดยมีมาตรการตามแนวปฏิบัติ ดังต่อไปนี้

๑) แนวปฏิบัติการควบคุมการเข้าถึงและใช้งานสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๒) นโยบายการจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ

กำหนดให้มีระบบสำรอง ระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

กำหนดผู้รับผิดชอบนโยบาย ดังนี้

๑) ผู้อำนวยการกองเทคโนโลยีดิจิทัล

๒) รองอธิการบดีผู้รับผิดชอบดูแลกองเทคโนโลยีดิจิทัล

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

โดยมีมาตรการตามแนวปฏิบัติ ดังนี้

๑) แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

๒) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๓) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

กำหนดผู้รับผิดชอบนโยบาย ดังนี้

๑) กองเทคโนโลยีดิจิทัล

๒) กองตรวจสอบภายใน หรือผู้ตรวจสอบจากภายนอก

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย/เจ้าหน้าที่ที่ได้รับมอบหมาย

โดยมีมาตรการตามแนวปฏิบัติ ดังนี้

๑) แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๔) นโยบายการสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

กำหนดให้มีการสร้างความรู้ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

กำหนดผู้รับผิดชอบนโยบาย ดังนี้

๑) ผู้อำนวยการกองเทคโนโลยีดิจิทัล

๒) ผู้อำนวยการกองการเจ้าหน้าที่

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

โดยมีมาตรการตามแนวปฏิบัติ ดังนี้

๑) แนวปฏิบัติการสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนด ในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อกำกับ ดูแลการดำเนินงาน การบริหารจัดการระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย โดยกำหนดเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังนี้

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๑) แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

(๑.๑) ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

(๑.๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

(๑.๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๑.๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

(๒) แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒.๑) การใช้บริการเครือข่าย

(๒.๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

(๒.๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

(๒.๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

(๒.๕) การแบ่งแยกเครือข่าย (Segregation in Networks)

(๒.๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

(๒.๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

(๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

(๔.๑) การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

(๔.๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

(๔.๓) การบริหารจัดการรหัสผ่าน (Password Management System)

(๔.๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

(๔.๕) การจำกัดระยะเวลาการใช้งานระบบสารสนเทศ (Session Time-Out)

(๔.๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection time)

(๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๕.๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

(๕.๒) การควบคุมการเข้าถึงระบบซึ่งไวต่อการรบกวน

(๕.๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารและการปฏิบัติงานจากภายนอกองค์กร (Mobile Compution and Teleworking)

(๕.๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๕.๕) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๑) แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

(๑.๑) การคัดเลือกและจัดทำระบบสำรอง

(๑.๒) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๑.๓) การกำหนดหน้าที่และความรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

(๑.๔) การทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉิน

(๒) แนวปฏิบัติการกู้คืนระบบ

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑) แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment)

(๒) การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยกองตรวจสอบภายใน (Internal Auditor) กองพัฒนาคุณภาพ เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศ เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

(๓) กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ปีละ ๑ ครั้ง

การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

(๑) แนวปฏิบัติการการสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

ข้อ ๕ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๖ มหาวิทยาลัยมีนโยบายไม่ตรวจตราการใช้เครือข่ายของผู้ใช้รายใดรายหนึ่งในกรณีปกติ แต่มหาวิทยาลัยสงวนสิทธิ์ในการติดตั้งเครื่องมือฮาร์ดแวร์หรือซอฟต์แวร์ เพื่อบันทึกและเฝ้าระวังการใช้คอมพิวเตอร์และเครือข่าย เพื่อคงไว้ซึ่งการให้บริการอย่างปลอดภัย มีประสิทธิภาพและเป็นไปตามกฎหมายบัญญัติ ทั้งนี้ มหาวิทยาลัยคงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้ระบบสารสนเทศ และดำเนินการสืบสวน เมื่อได้รับรายงาน การแจ้งเตือน หรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย ปัญหาเสถียรภาพ หรือการกระทำที่ขัดต่อนโยบายหรือพระราชบัญญัติมหาวิทยาลัย หรือกฎหมายของรัฐ

ข้อ ๗ กำหนดให้ “ผู้บริหารระดับสูงสุด” เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๘ กองเทคโนโลยีดิจิทัล มีหน้าที่ออกระเบียบปฏิบัติในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้เครือข่ายของผู้ฝ่าฝืนระเบียบ ตลอดจนระงับหรือจำกัดการเข้าถึงคอมพิวเตอร์ที่มีข้อมูลขัดต่อระเบียบ นโยบาย พระราชบัญญัติมหาวิทยาลัย หรือกฎหมายของรัฐ ในกรณีสำคัญให้กองเทคโนโลยีดิจิทัล รายงานการฝ่าฝืนระเบียบให้หน่วยงานต้นสังกัดและ/หรือมหาวิทยาลัยเพื่อพิจารณาลงโทษ

ข้อ ๙ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยแม่โจ้” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิสก์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ผู้ดูแลระบบผู้ใช้งาน ภายในมหาวิทยาลัยและหน่วยงานภายนอกต้องถือปฏิบัติอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ สิงหาคม พ.ศ. ๒๕๖๓

(รองศาสตราจารย์ ดร.วีระพล ทองมา)
อธิการบดีมหาวิทยาลัยแม่โจ้