ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

.....

ตามที่มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน ใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินการและกิจกรรมต่างๆ ซึ่งการใช้เทคโนโลยีสารสนเทศดังกล่าวอาจก่อให้เกิดความเสี่ยงในการดำเนินงานของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน และอาจก่อให้เกิดความเสียหายต่อการดำเนินกิจกรรมตามภารกิจของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสานได้ ดังนั้น เพื่อเป็นการป้องกันและควบคุมความเสี่ยงเกี่ยวกับการใช้เทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน จึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน ประกอบด้วย

๑) มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน นครราชสีมา

๒) มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน วิทยาเขตขอนแก่น

๓) มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน วิทยาเขตสุรินทร์

๔) มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน วิทยาเขตสกลนคร

“คณะกรรมการเทคโนโลยีสารสนเทศ” หมายความว่า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

“ระบบคอมพิวเตอร์และเครือข่าย” หมายความว่า ระบบคอมพิวเตอร์และเครือข่ายที่อยู่ภายใต้การดูแลและรับผิดชอบของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

“ระบบสารสนเทศ” หมายความว่า ระบบงานของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่สามารถ

นำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร

"สินทรัพย์" หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

"ผู้ใช้งาน" หมายความว่า บุคลากรและนักศึกษาของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

"ผู้ดูแลระบบ" หมายความว่า ข้าราชการพลเรือนในสถาบันอุดมศึกษา พนักงานในสถาบันอุดมศึกษา พนักงานราชการ ลูกจ้างประจำ หรือลูกจ้างเงินรายได้ ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย เพื่อจัดการฐานข้อมูลของระบบเครือข่าย

"จดหมายอิเล็กทรอนิกส์" หมายความว่า ระบบการรับส่งจดหมายข้อความระหว่างกันผ่านเครื่องคอมพิวเตอร์ ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ตามมาตรฐานที่ใช้ในการรับส่งข้อมูลได้แก่ SMTP, POP3 และ IMAP

"แบนด์วิดท์" หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่ สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

"บุคคลภายนอก" หมายความว่า บุคคลภายนอกมหาวิทยาลัยเทคโนโลยีราชมงคลอีสานแต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

"รหัสผ่าน" หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

"บัญชีผู้ใช้งาน หรือ บัญชีสมาชิกอินเทอร์เน็ต" หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

"เวลาอ้างอิงสากล" หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากลในประเทศไทยนั้นอ้างอิงกับหน่วยงาน

มาตรฐาน ได้แก่ กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"เลขที่อยู่ไอพี" หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

"เลขที่อยู่ไอพีสาธารณะ" หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

"ลงบันทึกเข้า" หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

"ลงบันทึกออก" หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจไม่คาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

"อุปกรณ์จัดเส้นทาง" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

"อุปกรณ์กระจายสัญญาณข้อมูล" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

"การพิสูจน์ยืนยันตัวตน" หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

"สิทธิ์" หมายความว่า สิทธิ์ผู้ใช้ สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง

ครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และ ความน่าเชื่อถือ (Reliability)

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"แผนผังระบบเครือข่าย" หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

ข้อ ๔ องค์ประกอบของนโยบาย

ส่วนที่ ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ของระบบคอมพิวเตอร์และเครือข่าย เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน และบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

ส่วนที่ ๒ การใช้ระบบคอมพิวเตอร์และระบบเครือข่าย เพื่อช่วยให้ผู้ใช้งานและบุคคลภายนอก ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูล ให้เป็นความลับมีความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ส่วนที่ ๓ การควบคุมการเข้าถึงระบบสารสนเทศ เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้คำนึงถึงการใช้งานและความมั่งคงปลอดภัย กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ การมอบอำนาจ และให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยให้มีการการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยของมหาวิทยาลัย

ส่วนที่ ๔ การควบคุมการเข้าถึงระบบเครือข่าย เพื่อควบคุมการเข้าถึงระบบเครือข่ายของมหาวิทยาลัย โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัย กำหนดกฎเกณฑ์ที่เกี่ยวกับการเข้าถึงระบบ

เครือข่าย ระบบเครือข่ายไร้สาย อุปกรณ์เชื่อมต่อเครือข่าย การป้องกันพอร์ต การแบ่งแยกเครือข่าย และการบริหารจัดการคอมพิวเตอร์แม่ข่าย

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อกำหนดการควบคุมการเข้าถึงระบบปฏิบัติการโดยกำหนดหน้าที่และแนวปฏิบัติ ขั้นตอน การบริหารจัดการรหัสผ่าน การใช้งานโปรแกรมอรรถประโยชน์ของผู้ดูแลและผู้ใช้งาน

ส่วนที่ ๖ การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศหรือแอพพลิเคชั่นและสารสนเทศ เพื่อควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และสามารถพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยได้อย่างถูกต้อง ในการเข้าใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน และป้องกันผู้บุรุกในการเข้าถึง โปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายกับระบบสารสนเทศหรือข้อมูลของมหาวิทยาลัย หรือทำให้การสื่อสารเสียหาย หยุดชะงัก

ส่วนที่ ๗ การปฏิบัติของผู้ดูแลระบบ เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย ในการบริหารจัดการกำกับดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) ให้สามารถใช้งานได้ดีอยู่เสมอ

ส่วนที่ ๘ การจัดทำระบบสำรองระบบสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่ายและเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินหรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของมหาวิทยาลัย

ส่วนที่ ๙ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

ส่วนที่ ๑๐ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ส่วนที่ ๑๑ การกำหนดผู้รับผิดชอบ เพื่อกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๕ จัดให้มีระบบบริหารความเสี่ยงของระบบสารสนเทศมหาวิทยาลัยเพื่อหาวิธีการป้องกันปัญหาอันจะส่งผลกระทบต่อระบบสารสนเทศของมหาวิทยาลัยและเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุน

การการบริหารงานของมหาวิทยาลัย แบบบูรณาการเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายต่อระบบสารสนเทศ

ข้อ ๖ ให้คณะกรรมการเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้และทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ จัดให้มีระบบเทคโนโลยีสารสนเทศและระบบสำรองข้อมูลสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อป้องกันผลกระทบที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ให้กลับคืนสู่สภาวะปกติ และสามารถปฏิบัติงานได้อย่างต่อเนื่อง

ข้อ ๘ ผู้ใช้งานทุกระดับจะต้องทราบและยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยโดยเคร่งครัด เพื่อให้ระบบสารสนเทศมีความมั่นคงและปลอดภัย ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ข้อบังคับ ประกาศ หรือคำสั่งใด ของมหาวิทยาลัย และข้อตกลงระหว่างประเทศอย่างเคร่งครัด หากผู้ใช้งานฝ่าฝืนจะต้องถูกลงโทษตามระเบียบ และกฎหมายที่เกี่ยวข้องต่อไป

ข้อ ๙ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๑๐ ให้อธิการบดีรักษาการให้เป็นไปตามประกาศนี้ และให้มีอำนาจตีความวินิจฉัยปัญหาอันเกิดจากการใช้ประกาศนี้

ประกาศ ณ วันที่ ๒๙ เดือน สิงหาคม พ.ศ. ๒๕๖๑

(ผู้ช่วยศาสตราจารย์วิโรจน์ ลิ้มไขแสง)

อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน