คู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ-มหาวิทยาลัยราชภัฏรำไพพรรณี

พ.ศ. ๒๕๖๙

(เอกสารแนบท้าย
ประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี
เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๙

จัดทำโดย
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏรำไพพรรณี

ผ่านความเห็นชอบ เมื่อวันที่ ๑๗ มิถุนายน ๒๕๖๙
จากคณะกรรมการจัดทำประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ
มหาวิทยาลัยราชภัฏรำไพพรรณี

บทนำ

มหาวิทยาลัยราชภัฏรำไพพรรณีตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งเป็นปัจจัยสำคัญในการสนับสนุนการดำเนินภารกิจของมหาวิทยาลัย ทั้งด้านการจัดการศึกษา การวิจัย การบริการวิชาการ การทำนุบำรุงศิลปวัฒนธรรม และการบริหารจัดการองค์กร โดยข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ และทรัพย์สินสารสนเทศต่าง ๆ ของมหาวิทยาลัยจำเป็นต้องได้รับการคุ้มครองและบริหารจัดการอย่างเหมาะสม เพื่อป้องกันความเสียหาย การเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต รวมถึงลดผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์และความเสี่ยงด้านสารสนเทศในรูปแบบต่าง ๆ

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มหาวิทยาลัยราชภัฏรำไพพรรณีจึงได้ออกประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ เพื่อกำหนดกรอบนโยบาย หลักการ และแนวทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

คู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จัดทำขึ้นเป็นเอกสารแนบท้ายประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ เพื่อกำหนดรายละเอียด หลักเกณฑ์ แนวทางปฏิบัติ มาตรการควบคุม และขั้นตอนการดำเนินงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม เป็นมาตรฐานเดียวกัน และสอดคล้องกับนโยบายที่มหาวิทยาลัยกำหนด

คู่มือฉบับนี้ใช้บังคับกับบุคลากร นักศึกษา ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้รับจ้าง ผู้ให้บริการภายนอก ตลอดจนบุคคลใดที่ได้รับอนุญาตให้เข้าถึง ใช้งาน หรือเกี่ยวข้องกับข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ หรือทรัพย์สินสารสนเทศของมหาวิทยาลัย โดยทุกฝ่ายมีหน้าที่ต้องศึกษา ทำความเข้าใจ และถือปฏิบัติตามประกาศมหาวิทยาลัยและคู่มือฉบับนี้อย่างเคร่งครัด

เนื้อหาในคู่มือฉบับนี้ครอบคลุมแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในประเด็นสำคัญต่าง ๆ ได้แก่ การบริหารจัดการสินทรัพย์สารสนเทศ การควบคุมการเข้าถึงระบบและข้อมูล การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การบริหารจัดการเครือข่ายและระบบสารสนเทศ การสำรองและกู้คืนข้อมูล การเฝ้าระวังและรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการปฏิบัติตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

ในกรณีที่มีรายละเอียดทางเทคนิค วิธีปฏิบัติงาน หรือมาตรการเฉพาะด้านที่จำเป็นต่อการดำเนินงาน ให้หน่วยงานที่รับผิดชอบจัดทำแนวปฏิบัติหรือคู่มือปฏิบัติงานเพิ่มเติมได้ตามความเหมาะสม ทั้งนี้ ต้องไม่ขัดหรือแย้งกับประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ และคู่มือฉบับนี้

๑. วัตถุประสงค์ (Objectives)

คู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อกำหนดรายละเอียด หลักเกณฑ์ แนวทางปฏิบัติ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยราชภัฏรำไพพรรณี ให้เป็นไปตามประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑ เพื่อกำหนดแนวทางและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยให้เป็นมาตรฐานเดียวกัน

๑.๒ เพื่อปกป้องข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ และทรัพย์สินสารสนเทศของมหาวิทยาลัยจากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง การทำลาย หรือการใช้งานโดยไม่ได้รับอนุญาต

๑.๓ เพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศและระบบสารสนเทศของมหาวิทยาลัย

๑.๔ เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในการใช้งาน ดูแล และบริหารจัดการระบบสารสนเทศและข้อมูลสารสนเทศของมหาวิทยาลัย

๑.๕ เพื่อส่งเสริมให้บุคลากร นักศึกษา ผู้ปฏิบัติงาน ผู้รับจ้าง ผู้ให้บริการภายนอก และผู้ที่เกี่ยวข้อง มีความตระหนักรู้และปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

๑.๖ เพื่อสนับสนุนการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดที่เกี่ยวข้อง

๑.๗ เพื่อสนับสนุนความต่อเนื่องในการดำเนินภารกิจของมหาวิทยาลัย (Business Continuity) และความสามารถในการกู้คืนระบบสารสนเทศเมื่อเกิดเหตุขัดข้องหรือสถานการณ์ฉุกเฉิน

๒. ขอบเขต (Scope)

คู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ใช้บังคับกับบุคคล หน่วยงาน ระบบเทคโนโลยีสารสนเทศ ข้อมูลสารสนเทศ และทรัพย์สินสารสนเทศที่อยู่ภายใต้ความรับผิดชอบของมหาวิทยาลัยราชภัฏรำไพพรรณี โดยครอบคลุมรายละเอียดดังต่อไปนี้

๒.๑ บุคคลที่อยู่ภายใต้การบังคับใช้

(๑) ผู้บริหารมหาวิทยาลัย

(๒) บุคลากรของมหาวิทยาลัยทุกประเภท

(๓) พนักงานราชการ พนักงานมหาวิทยาลัย ลูกจ้างประจำ และลูกจ้างชั่วคราว

(๔) นักศึกษา

(๕) ผู้ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

(๖) ผู้ปฏิบัติงานที่ได้รับมอบหมายให้เข้าถึงข้อมูลหรือระบบสารสนเทศของมหาวิทยาลัย

(๗) ผู้รับจ้าง ผู้ให้บริการ ผู้พัฒนาระบบ ผู้ให้บริการระบบคลาวด์ และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบสารสนเทศของมหาวิทยาลัย

(๘) บุคคลหรือหน่วยงานอื่นใดที่ได้รับอนุญาตให้ใช้งานหรือเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๒.๒ ขอบเขตด้านข้อมูลและทรัพย์สินสารสนเทศ

(๑) ข้อมูลสารสนเทศของมหาวิทยาลัยในทุกรูปแบบ ทั้งข้อมูลอิเล็กทรอนิกส์ ข้อมูลที่จัดเก็บในระบบสารสนเทศ และเอกสารที่อยู่ในรูปแบบกระดาษ

(๒) ข้อมูลส่วนบุคคล ข้อมูลทางการศึกษา ข้อมูลการบริหารจัดการ และข้อมูลอื่นที่อยู่ในความครอบครองหรือความรับผิดชอบของมหาวิทยาลัย

(๓) ฐานข้อมูล ระบบจัดเก็บข้อมูล และสื่อบันทึกข้อมูลทุกประเภท

(๔) ทรัพย์สินสารสนเทศอื่นที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย

๒.๓ ขอบเขตด้านระบบและเทคโนโลยีสารสนเทศ

(๑) ระบบเทคโนโลยีสารสนเทศทั้งหมดของมหาวิทยาลัย

(๒) ระบบสารสนเทศเพื่อการบริหาร การจัดการศึกษา การวิจัย และการบริการวิชาการ

(๓) ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์เครือข่ายทุกประเภท

(๔) เครื่องคอมพิวเตอร์ เครื่องแม่ข่าย อุปกรณ์เคลื่อนที่ และอุปกรณ์ดิจิทัลที่เชื่อมต่อกับระบบของมหาวิทยาลัย

(๕) ระบบจดหมายอิเล็กทรอนิกส์ เว็บไซต์ ระบบคลาวด์ และบริการดิจิทัลอื่นที่มหาวิทยาลัยเป็นเจ้าของ เช่าใช้ หรืออยู่ภายใต้การกำกับดูแล

(๖) ระบบหรือบริการของหน่วยงานภายนอกที่เชื่อมต่อหรือมีการแลกเปลี่ยนข้อมูลกับมหาวิทยาลัย

๒.๔ ขอบเขตด้านสถานที่และสิ่งอำนวยความสะดวก

(๑) ศูนย์ข้อมูล (Data Center)

(๒) ห้องปฏิบัติการคอมพิวเตอร์

(๓) ห้องควบคุมระบบเครือข่าย

(๔) พื้นที่ติดตั้งอุปกรณ์สารสนเทศและอุปกรณ์เครือข่าย

(๕) สถานที่หรือพื้นที่ที่ใช้จัดเก็บข้อมูลหรือทรัพย์สินสารสนเทศของมหาวิทยาลัย

๒.๕ ขอบเขตการบังคับใช้

คู่มือฉบับนี้ให้ใช้บังคับกับการเข้าถึง การใช้งาน การจัดเก็บ การประมวลผล การส่งต่อ การเปิดเผย การสำรองข้อมูล การกู้คืนข้อมูล และการบริหารจัดการข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ และทรัพย์สินสารสนเทศของมหาวิทยาลัย ทั้งที่ดำเนินการภายในมหาวิทยาลัยและผ่านระบบหรือบริการของหน่วยงานภายนอกที่เกี่ยวข้อง

ทั้งนี้ ผู้ที่อยู่ภายใต้ขอบเขตตามคู่มือฉบับนี้ต้องถือปฏิบัติตามประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ และคู่มือฉบับนี้อย่างเคร่งครัด

๓. กฎหมายและข้อกำหนดที่เกี่ยวข้อง (Legal and Regulatory Compliance)

คู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จัดทำขึ้นโดยอ้างอิงและสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง ดังต่อไปนี้

๓.๑ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

๓.๒ พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๓.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒ ๕๖๐ และที่แก้ไขเพิ่มเติม

๓.๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๕ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓.๖ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และที่แก้ไขเพิ่มเติม

๓.๗ ประกาศ ระเบียบ และแนวปฏิบัติที่ออกตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๘ ประกาศ ระเบียบ และแนวปฏิบัติที่ออกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓.๙ ประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙

๓.๑๐ ระเบียบ ข้อบังคับ คำสั่ง ประกาศ และแนวปฏิบัติอื่นของมหาวิทยาลัยราชภัฏรำไพพรรณีที่เกี่ยวข้องกับการบริหารจัดการเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๓.๑๑ สัญญา ข้อตกลงการให้บริการ (Service Agreement) ข้อตกลงการรักษาความลับ (Non-Disclosure Agreement) และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่มหาวิทยาลัยทำไว้กับหน่วยงานหรือผู้ให้บริการภายนอก

ในกรณีที่มีการแก้ไขเพิ่มเติมกฎหมาย ระเบียบ ประกาศ หรือข้อกำหนดใดที่เกี่ยวข้อง ให้ถือปฏิบัติตามฉบับที่มีผลใช้บังคับในปัจจุบัน และให้มีการทบทวนคู่มือฉบับนี้ตามความเหมาะสม

๔. บทบาทและหน้าที่ของผู้ที่เกี่ยวข้อง

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยราชภัฏรำไพพรรณีเป็นไปอย่างมีประสิทธิภาพ ผู้ที่เกี่ยวข้องทุกฝ่ายต้องมีบทบาท หน้าที่ และความรับผิดชอบในการปฏิบัติตามประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ และคู่มือฉบับนี้ ดังต่อไปนี้

๔.๑ อธิการบดี

(๑) กำกับดูแลและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย

(๒) อนุมัติประกาศ นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

(๓) สนับสนุนทรัพยากรที่จำเป็นสำหรับการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ

(๔) กำกับติดตามให้หน่วยงานในมหาวิทยาลัยดำเนินการตามนโยบายและแนวปฏิบัติที่กำหนด

๔.๒ ศูนย์เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๑) รับผิดชอบการบริหารจัดการระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานด้านสารสนเทศของมหาวิทยาลัย

(๒) จัดทำ ทบทวน และปรับปรุงคู่มือนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

(๓) ให้คำปรึกษา สนับสนุน และประสานงานด้านความมั่นคงปลอดภัยสารสนเทศแก่หน่วยงานต่าง ๆ

(๔) ติดตาม เฝ้าระวัง และประสานการดำเนินการเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(๕) ส่งเสริมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรและนักศึกษา

๔.๓ หน่วยงานเจ้าของระบบสารสนเทศ

(๑) กำกับดูแลระบบสารสนเทศที่อยู่ในความรับผิดชอบให้เป็นไปตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

(๒) กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบตามความจำเป็นในการปฏิบัติงาน

(๓) ประสานงานกับสำนักวิทยบริการและเทคโนโลยีสารสนเทศในการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ

(๔) แจ้งเหตุการณ์หรือความผิดปกติที่อาจส่งผลกระทบต่อระบบสารสนเทศให้หน่วยงานที่เกี่ยวข้องทราบโดยเร็ว

๔.๔ หน่วยงานเจ้าของข้อมูล

(๑) กำกับดูแลข้อมูลที่อยู่ในความรับผิดชอบให้ได้รับการคุ้มครองอย่างเหมาะสม

(๒) กำหนดระดับการเข้าถึงข้อมูลตามความจำเป็นในการปฏิบัติงาน

(๓) ตรวจสอบความถูกต้อง ความครบถ้วน และความเหมาะสมของการใช้ข้อมูล

(๔) ประสานงานกับหน่วยงานที่เกี่ยวข้องในการป้องกันและแก้ไขปัญหาที่อาจส่งผลกระทบต่อข้อมูลสารสนเทศ

๔.๕ ผู้ดูแลระบบ

(๑) ดูแล ควบคุม และบำรุงรักษาระบบที่ได้รับมอบหมาย

(๒) ดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่มหาวิทยาลัยกำหนด

(๓) ควบคุมสิทธิ์การเข้าถึงระบบให้เป็นไปตามที่ได้รับอนุมัติ

(๔) เฝ้าระวัง ตรวจสอบ และรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่พบ

(๕) สำรองข้อมูลและดำเนินการกู้คืนระบบตามแนวทางที่กำหนด

๔.๖ บุคลากร นักศึกษา และผู้ใช้งานระบบ

(๑) ศึกษา ทำความเข้าใจ และปฏิบัติตามประกาศ นโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย

(๒) ใช้งานระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

(๓) รักษาความลับของบัญชีผู้ใช้งาน รหัสผ่าน และข้อมูลที่อยู่ในความรับผิดชอบ

(๔) แจ้งเหตุการณ์หรือความผิดปกติด้านความมั่นคงปลอดภัยสารสนเทศต่อหน่วยงานที่รับผิดชอบโดยเร็ว

(๕) หลีกเลี่ยงการกระทำที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ข้อมูลสารสนเทศ หรือเครือข่ายของมหาวิทยาลัย

๔.๗ ผู้รับจ้าง ผู้ให้บริการ และบุคคลภายนอก

(๑) ปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่มหาวิทยาลัยกำหนด

(๒) ใช้ข้อมูลและระบบสารสนเทศเฉพาะตามขอบเขตที่ได้รับอนุญาต

(๓) รักษาความลับของข้อมูลและทรัพย์สินสารสนเทศของมหาวิทยาลัย

(๔) แจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องให้มหาวิทยาลัยทราบโดยทันที

(๕) รับผิดชอบต่อความเสียหายที่เกิดจากการกระทำที่ฝ่าฝืนข้อกำหนดหรือสัญญาที่เกี่ยวข้อง

๕. คำนิยาม (Definitions)

เพื่อให้การตีความและการปฏิบัติตามคู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นไปในทิศทางเดียวกัน มหาวิทยาลัยราชภัฏรำไพพรรณีกำหนดคำนิยามที่เกี่ยวข้อง ดังต่อไปนี้

๕.๑ ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)

หมายถึง การดำเนินการเพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ ระบบสารสนเทศ และทรัพย์สินสารสนเทศ รวมถึงการป้องกันการเข้าถึง การใช้งาน การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต

๕.๒ ข้อมูลสารสนเทศ (Information)

หมายถึง ข้อมูล ข่าวสาร เอกสาร หรือเนื้อหาในรูปแบบใด ๆ ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์หรือรูปแบบกายภาพ รวมถึงข้อมูลที่มีการจัดเก็บ ประมวลผล รับ ส่ง แลกเปลี่ยน หรือเผยแพร่ด้วยวิธีการใด ๆ ซึ่งอยู่ในความครอบครอง การควบคุมดูแล หรือความรับผิดชอบของมหาวิทยาลัย และใช้ในการดำเนินงานตามภารกิจของมหาวิทยาลัย

๕.๓ ทรัพย์สินสารสนเทศ (Information Asset)

หมายถึง ข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ โปรแกรมคอมพิวเตอร์ ฐานข้อมูล อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย สื่อบันทึกข้อมูล เอกสาร บริการดิจิทัล บริการคลาวด์ ตลอดจนทรัพยากรหรือองค์ประกอบอื่นใดที่เกี่ยวข้องกับการสร้าง การประมวลผล การจัดเก็บ การรับ ส่ง การ

แลกเปลี่ยน การเผยแพร่ หรือการใช้งานข้อมูลสารสนเทศ ซึ่งอยู่ในความครอบครอง การควบคุมดูแล หรือความรับผิดชอบของมหาวิทยาลัย และมีคุณค่าต่อการดำเนินงานตามภารกิจของมหาวิทยาลัย

๕.๔ ระบบสารสนเทศ (Information System)

หมายถึง ระบบที่ประกอบด้วยบุคลากร กระบวนการปฏิบัติงาน ข้อมูลสารสนเทศ และเทคโนโลยีที่เกี่ยวข้อง ซึ่งทำงานร่วมกันเพื่อรวบรวม ประมวลผล จัดเก็บ รับ ส่ง แลกเปลี่ยน หรือเผยแพร่ข้อมูลสารสนเทศ เพื่อสนับสนุนการดำเนินงาน การบริหารจัดการ การจัดการศึกษา การวิจัย และภารกิจอื่นของมหาวิทยาลัย

๕.๕ ระบบเทคโนโลยีสารสนเทศ (Information Technology System)

หมายถึง อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย โปรแกรมคอมพิวเตอร์ ระบบปฏิบัติการ ระบบฐานข้อมูล บริการดิจิทัล บริการคลาวด์ และทรัพยากรด้านเทคโนโลยีสารสนเทศอื่นที่ใช้ในการสนับสนุนการดำเนินงาน การบริหารจัดการ และภารกิจของมหาวิทยาลัย

๕.๖ ระบบเครือข่ายคอมพิวเตอร์ (Computer Network)

หมายถึง ระบบการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศ และระบบสารสนเทศ เพื่อการรับ ส่ง แลกเปลี่ยนข้อมูล และการสื่อสารทั้งภายในและภายนอกมหาวิทยาลัย

๕.๗ ผู้ดูแลระบบ (System Administrator)

หมายถึง บุคลากรหรือผู้ที่ได้รับมอบหมายจากมหาวิทยาลัยให้มีหน้าที่ดูแล บริหารจัดการ ควบคุม บำรุงรักษา หรือกำกับการใช้งานระบบสารสนเทศ ระบบเครือข่าย ระบบเทคโนโลยีสารสนเทศ หรือทรัพยากรสารสนเทศที่อยู่ในความรับผิดชอบ

๕.๘ ผู้ใช้งาน (User)

หมายถึง บุคลากร นักศึกษา ผู้รับจ้าง ผู้ให้บริการภายนอก หรือบุคคลใดที่ได้รับอนุญาตให้เข้าถึง ใช้งาน หรือเกี่ยวข้องกับข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย

๕.๙ สิทธิการเข้าถึง (Access Rights)

หมายถึง สิทธิหรือระดับการอนุญาตที่กำหนดให้บุคคลสามารถเข้าถึง ใช้งาน เพิ่ม แก้ไข เปลี่ยนแปลง ลบ หรือดำเนินการอื่นใดกับข้อมูลสารสนเทศ ระบบสารสนเทศ หรือทรัพยากรสารสนเทศ ตามบทบาท หน้าที่ และความจำเป็นในการปฏิบัติงานที่ได้รับมอบหมาย

๕.๑๐ เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident)
หมายถึง เหตุการณ์ การกระทำ หรือสถานการณ์ที่เกิดขึ้นแล้ว หรืออาจก่อให้เกิดผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) หรือความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือทรัพย์สินสารสนเทศของมหาวิทยาลัย

๕.๑๑ การตรวจสอบย้อนหลัง (Audit Trail)
หมายถึง ข้อมูลบันทึกเหตุการณ์ กิจกรรม หรือการดำเนินการที่เกิดขึ้นในระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย ซึ่งสามารถใช้ในการตรวจสอบ วิเคราะห์ ติดตาม ระบุผู้ใช้งาน และพิสูจน์เหตุการณ์ที่เกิดขึ้นย้อนหลังได้

๕.๑๒ ข้อมูลส่วนบุคคล (Personal Data)
หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ทั้งนี้ ให้มีความหมายตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม

๕.๑๓ บุคคลภายนอก (Third Party)
หมายถึง บุคคล หน่วยงาน องค์กร ผู้รับจ้าง ผู้ให้บริการ หรือผู้มีส่วนเกี่ยวข้องอื่นใด ที่มิใช่บุคลากรหรือนักศึกษาของมหาวิทยาลัย แต่ได้รับอนุญาตให้เข้าถึง ใช้งาน เชื่อมต่อ หรือเกี่ยวข้องกับข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือทรัพย์สินสารสนเทศของมหาวิทยาลัย

๕.๑๔ บัญชีผู้ใช้งาน (User Account)
หมายถึง ชุดข้อมูลที่ใช้สำหรับระบุตัวตนและกำหนดสิทธิการเข้าถึงของผู้ใช้งานในการเข้าใช้งานระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือบริการดิจิทัลของมหาวิทยาลัย ซึ่งอาจประกอบด้วยชื่อผู้ใช้งาน (Username) รหัสประจำตัวผู้ใช้งาน (User ID) รหัสผ่าน (Password) หรือข้อมูลอื่นที่ใช้ในการพิสูจน์ตัวตน

๕.๑๕ การพิสูจน์ตัวตน (Authentication)
หมายถึง กระบวนการตรวจสอบและยืนยันตัวตนของผู้ใช้งาน ระบบ หรืออุปกรณ์ ก่อนอนุญาตให้เข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือทรัพย์สินสารสนเทศของมหาวิทยาลัย

๕.๑๖ บันทึกเหตุการณ์ (Log)
หมายถึง ข้อมูลที่ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เครือข่าย หรืออุปกรณ์ที่เกี่ยวข้องบันทึกไว้เกี่ยวกับเหตุการณ์ กิจกรรม หรือการดำเนินการต่าง ๆ ที่เกิดขึ้นในระบบ เพื่อใช้ในการติดตาม ตรวจสอบ วิเคราะห์ เฝ้าระวัง หรือสนับสนุนการตรวจสอบย้อนหลัง โดยอาจนำมาใช้เป็นส่วนหนึ่งของข้อมูลสำหรับการจัดทำการตรวจสอบย้อนหลัง (Audit Trail)

๕.๑๗ บริการคลาวด์ (Cloud Service)
หมายถึง บริการด้านเทคโนโลยีสารสนเทศที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายสื่อสารอื่น โดยผู้ใช้งานสามารถเข้าถึงทรัพยากรด้านคอมพิวเตอร์ ซอฟต์แวร์ พื้นที่จัดเก็บข้อมูล ระบบประมวลผล หรือบริการดิจิทัลต่าง ๆ ได้ตามสิทธิที่ได้รับอนุญาต โดยไม่จำเป็นต้องเป็นเจ้าของหรือบริหารจัดการโครงสร้างพื้นฐานดังกล่าวโดยตรง

๕.๑๘ เจ้าของข้อมูล (Data Owner)

หมายถึง หน่วยงานหรือผู้ที่ได้รับมอบหมายจากมหาวิทยาลัยให้มีอำนาจหน้าที่รับผิดชอบในการกำกับดูแล ควบคุม และบริหารจัดการข้อมูลสารสนเทศที่อยู่ในความรับผิดชอบของตน รวมถึงการกำหนดระดับชั้นความลับ การกำหนดสิทธิการเข้าถึง การกำหนดแนวทางการใช้งาน การเปิดเผย การจัดเก็บ การส่งต่อ และการทำลายข้อมูลให้เป็นไปตามกฎหมาย ระเบียบ นโยบาย และข้อกำหนดที่เกี่ยวข้อง

๕.๑๙ เจ้าของระบบ (System Owner)

หมายถึง หน่วยงานหรือผู้ที่ได้รับมอบหมายจากมหาวิทยาลัยให้มีอำนาจหน้าที่รับผิดชอบในการกำกับดูแล บริหารจัดการ และควบคุมการดำเนินงานของระบบสารสนเทศหรือระบบเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบ รวมถึงการกำหนดสิทธิการเข้าถึง การกำหนดความต้องการด้านความมั่นคงปลอดภัย การบริหารความเสี่ยง การควบคุมการเปลี่ยนแปลง และการติดตามให้ระบบสามารถดำเนินงานได้อย่างถูกต้อง มั่นคงปลอดภัย และสอดคล้องกับภารกิจของมหาวิทยาลัย

๕.๒๐ ระดับชั้นความลับของข้อมูล (Information Classification)

หมายถึง การจัดประเภทข้อมูลสารสนเทศตามระดับความสำคัญ ความอ่อนไหว และผลกระทบที่อาจเกิดขึ้นต่อมหาวิทยาลัย เจ้าของข้อมูล หรือผู้มีส่วนเกี่ยวข้อง หากข้อมูลดังกล่าวถูกเปิดเผย แก้ไข เปลี่ยนแปลง สูญหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต โดยมหาวิทยาลัยอาจกำหนดระดับชั้นความลับของข้อมูลตามความเหมาะสม เพื่อใช้เป็นเกณฑ์ในการกำหนดมาตรการควบคุม การเข้าถึง การใช้งาน การจัดเก็บ การส่งต่อ การเผยแพร่ และการทำลายข้อมูลสารสนเทศ

๖. หมวดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยราชภัฏรำไพพรรณีเป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ และกฎหมายที่เกี่ยวข้อง มหาวิทยาลัยจึงกำหนดหมวดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

๖.๑ นโยบายการบริหารจัดการสินทรัพย์สารสนเทศและการรักษาความลับ

วัตถุประสงค์

เพื่อให้ข้อมูลสารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัยได้รับการจำแนกประเภท ควบคุม ดูแล และคุ้มครองอย่างเหมาะสมตามระดับความสำคัญและระดับชั้นความลับของข้อมูล

นโยบาย

มหาวิทยาลัยกำหนดให้มีการบริหารจัดการสินทรัพย์สารสนเทศและการรักษาความลับของข้อมูลตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การเปิดเผย การส่งต่อ การสำรองข้อมูล และการทำลายข้อมูล โดยต้องมีมาตรการคุ้มครองข้อมูลและทรัพย์สินสารสนเทศให้เป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

แนวปฏิบัติ

การระบุและขึ้นทะเบียนทรัพย์สินสารสนเทศ

(๑) หน่วยงานต้องจัดทำทะเบียนทรัพย์สินสารสนเทศที่อยู่ในความรับผิดชอบให้เป็นปัจจุบัน

(๒) ทรัพย์สินสารสนเทศที่ต้องขึ้นทะเบียนอย่างน้อย ได้แก่ ข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย สื่อบันทึกข้อมูล บริการดิจิทัล และบริการคลาวด์

(๓) ทรัพย์สินสารสนเทศแต่ละรายการต้องกำหนดผู้รับผิดชอบหรือเจ้าของทรัพย์สินสารสนเทศอย่างชัดเจน

(๔) ต้องมีการทบทวนทะเบียนทรัพย์สินสารสนเทศอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

การกำหนดเจ้าของข้อมูลและเจ้าของระบบ

(๑) ข้อมูลสารสนเทศทุกประเภทต้องมีการกำหนดเจ้าของข้อมูล (Data Owner)

(๒) ระบบสารสนเทศและระบบเทคโนโลยีสารสนเทศทุกระบบต้องมีการกำหนดเจ้าของระบบ (System Owner)

(๓) เจ้าของข้อมูลมีหน้าที่กำหนดระดับชั้นความลับ สิทธิการเข้าถึง และแนวทางการใช้ข้อมูล รวมถึงทบทวนสิทธิการเข้าถึงข้อมูลอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ

(๔) เจ้าของระบบมีหน้าที่กำกับดูแลการใช้งานและความมั่นคงปลอดภัยของระบบที่รับผิดชอบ

การจำแนกประเภทและกำหนดระดับชั้นความลับของข้อมูล

(๑) ข้อมูลสารสนเทศต้องได้รับการจำแนกประเภทและกำหนดระดับชั้นความลับตามความสำคัญ ความอ่อนไหว และผลกระทบที่อาจเกิดขึ้นหากข้อมูลถูกเปิดเผย สูญหาย หรือถูกแก้ไขโดยไม่ได้รับอนุญาต

(๒) มหาวิทยาลัยกำหนดระดับชั้นความลับของข้อมูล ดังนี้

ก. ข้อมูลสาธารณะ (Public)

ข. ข้อมูลสำหรับใช้ภายใน (Internal Use)

ค. ข้อมูลลับ (Confidential)

ง. ข้อมูลลับมาก (Highly Confidential) หรือระดับชั้นความลับอื่นตามที่มหาวิทยาลัยกำหนด

(๓) เจ้าของข้อมูลต้องเป็นผู้กำหนดและทบทวนระดับชั้นความลับของข้อมูลอย่างเหมาะสม

การจัดเก็บและการใช้งานข้อมูลสารสนเทศ

(๑) การจัดเก็บข้อมูลสารสนเทศต้องสอดคล้องกับระดับชั้นความลับของข้อมูล

(๒) ต้องมีมาตรการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๓) ผู้ใช้งานต้องใช้ข้อมูลสารสนเทศตามวัตถุประสงค์ที่ได้รับอนุญาตเท่านั้น

(๔) ห้ามคัดลอก เปิดเผย ส่งต่อ หรือเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้มีอำนาจ

การรับ ส่ง และแลกเปลี่ยนข้อมูลสารสนเทศ

(๑) การรับ ส่ง หรือแลกเปลี่ยนข้อมูลสารสนเทศต้องดำเนินการผ่านช่องทางที่เหมาะสมและมีมาตรการรักษาความมั่นคงปลอดภัย

(๒) กรณีเป็นข้อมูลส่วนบุคคลหรือข้อมูลลับ ต้องมีมาตรการป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(๓) การเปิดเผยข้อมูลแก่บุคคลภายนอกต้องได้รับอนุมัติตามอำนาจหน้าที่และเป็นไปตามกฎหมายที่เกี่ยวข้อง

การจัดเก็บรักษาและการทำลายข้อมูล

(๑) ข้อมูลสารสนเทศต้องได้รับการจัดเก็บรักษาตามระยะเวลาที่กำหนดไว้ในกฎหมาย ระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง

(๒) เมื่อพ้นระยะเวลาการจัดเก็บหรือไม่มีความจำเป็นต้องใช้งานแล้ว ต้องดำเนินการทำลายข้อมูลด้วยวิธีการที่เหมาะสมและปลอดภัย

(๓) การทำลายข้อมูลต้องสามารถป้องกันการกู้คืนหรือการนำข้อมูลกลับมาใช้ได้โดยไม่ได้รับอนุญาต

(๔) ต้องมีหลักฐานหรือบันทึกการทำลายข้อมูลตามความเหมาะสม

การจัดการสื่อบันทึกข้อมูล

(๑) สื่อบันทึกข้อมูลทุกประเภทที่ใช้ในการจัดเก็บข้อมูลสารสนเทศของมหาวิทยาลัย เช่น ฮาร์ดดิสก์ภายนอก (External Hard Disk) แฟลชไดรฟ์ (USB Flash Drive) แผ่นบันทึกข้อมูล หรือสื่อบันทึกข้อมูลประเภทอื่น ต้องได้รับการควบคุมและคุ้มครองตามระดับชั้นความลับของข้อมูลที่จัดเก็บอยู่ในสื่อนั้น

(๒) การใช้งาน การเคลื่อนย้าย การจัดเก็บ หรือการนำสื่อบันทึกข้อมูลออกนอกพื้นที่ควบคุมของมหาวิทยาลัย ต้องได้รับอนุญาตจากผู้มีอำนาจหรือผู้รับผิดชอบตามที่มหาวิทยาลัยกำหนด

(๓) สื่อบันทึกข้อมูลที่ใช้จัดเก็บข้อมูลลับ ข้อมูลลับมาก หรือข้อมูลส่วนบุคคล ต้องมีมาตรการป้องกันที่เหมาะสม เช่น การเข้ารหัสข้อมูล การกำหนดสิทธิการเข้าถึง หรือมาตรการอื่นตามความเหมาะสม

(๔) เมื่อสื่อบันทึกข้อมูลหมดความจำเป็นในการใช้งาน ชำรุด หรือสิ้นสุดอายุการใช้งาน ต้องดำเนินการลบ ทำลาย หรือกำจัดข้อมูลและสื่อบันทึกข้อมูลด้วยวิธีการที่ปลอดภัย เพื่อป้องกันการเข้าถึงหรือการกู้คืนข้อมูลโดยไม่ได้รับอนุญาต

การส่งมอบและการคืนทรัพย์สินสารสนเทศ

(๑) บุคลากร นักศึกษา ผู้รับจ้าง ผู้ให้บริการ หรือบุคคลภายนอกที่ได้รับมอบหมายให้ใช้หรือครอบครองทรัพย์สินสารสนเทศของมหาวิทยาลัย ต้องรับผิดชอบดูแลทรัพย์สินสารสนเทศดังกล่าวตามหน้าที่และระยะเวลาที่ได้รับมอบหมาย

(๒) เมื่อมีการเปลี่ยนแปลงตำแหน่งหน้าที่ การโยกย้าย การลาออก การพ้นสภาพ การสิ้นสุดสัญญาหรือสิ้นสุดความจำเป็นในการใช้งาน ต้องดำเนินการส่งคืนทรัพย์สินสารสนเทศ บัญชีผู้ใช้งาน เอกสาร สื่อบันทึกข้อมูล และข้อมูลที่อยู่ในความรับผิดชอบให้แก่หน่วยงานที่เกี่ยวข้อง รวมถึงอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสาร อุปกรณ์จัดเก็บข้อมูล และทรัพย์สินสารสนเทศอื่นที่ได้รับมอบหมาย

(๓) หน่วยงานผู้รับผิดชอบต้องตรวจสอบความครบถ้วน ความถูกต้อง และสภาพของทรัพย์สินสารสนเทศก่อนรับคืน และดำเนินการเพิกถอนหรือปรับปรุงสิทธิการเข้าถึงระบบตามความเหมาะสม

(๔) การส่งมอบหรือส่งคืนทรัพย์สินสารสนเทศต้องมีการบันทึกหรือจัดทำหลักฐานประกอบการดำเนินการตามที่มหาวิทยาลัยกำหนด

การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสำคัญ

(๑) การเก็บรวบรวม ใช้ เปิดเผย หรือประมวลผลข้อมูลส่วนบุคคล ต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายที่เกี่ยวข้อง

(๒) ข้อมูลสำคัญของมหาวิทยาลัยต้องได้รับการคุ้มครองตามระดับความเสี่ยงและระดับชั้นความลับที่กำหนด

(๓) หน่วยงานต้องกำหนดมาตรการป้องกันการรั่วไหล การสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๔) กรณีพบเหตุการณ์ละเมิดข้อมูล ต้องดำเนินการตามนโยบายการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย

<u>การรักษาความลับของข้อมูล</u>

(๑) ผู้ใช้งานทุกคนต้องรักษาความลับของข้อมูลสารสนเทศที่อยู่ในความรับผิดชอบ และต้องไม่นำข้อมูลไปใช้ เปิดเผย คัดลอก ส่งต่อ หรือเผยแพร่แก่บุคคลที่ไม่มีสิทธิได้รับข้อมูลดังกล่าว

(๒) การเข้าถึง ใช้งาน หรือเปิดเผยข้อมูลสารสนเทศ ต้องเป็นไปตามอำนาจหน้าที่ ความจำเป็นในการปฏิบัติงาน และระดับชั้นความลับของข้อมูล

(๓) บุคลากร ผู้รับจ้าง ผู้ให้บริการ หรือบุคคลภายนอกที่มีสิทธิเข้าถึงข้อมูลสำคัญ ข้อมูลลับ ข้อมูลลับมาก หรือข้อมูลส่วนบุคคล ต้องลงนามในข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA) หรือเอกสารอื่นที่มหาวิทยาลัยกำหนด

(๔) ห้ามเปิดเผยข้อมูลสารสนเทศของมหาวิทยาลัยต่อสาธารณะหรือบุคคลภายนอก เว้นแต่ได้รับอนุญาตจากผู้มีอำนาจ หรือเป็นการดำเนินการตามกฎหมาย ระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง

(๕) กรณีพบหรือสงสัยว่ามีการเปิดเผยข้อมูล การรั่วไหลของข้อมูล หรือการละเมิดความลับของข้อมูล ต้องรายงานต่อหน่วยงานที่รับผิดชอบโดยทันที และดำเนินการตามนโยบายการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย

๖.๒ นโยบายการควบคุมการเข้าถึงและการพิสูจน์ตัวตน

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต และเพื่อให้สามารถตรวจสอบตัวตนของผู้ใช้งานได้อย่างเหมาะสม

นโยบาย

มหาวิทยาลัยกำหนดให้มีการควบคุมการเข้าถึงข้อมูล ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศและบริการดิจิทัลตามบทบาทหน้าที่และความจำเป็นในการปฏิบัติงาน โดยต้องมีการพิสูจน์ตัวตน การกำหนดสิทธิการเข้าถึง และการบริหารจัดการบัญชีผู้ใช้งานอย่างเหมาะสม

แนวปฏิบัติ

<u>การบริหารจัดการบัญชีผู้ใช้งาน (User Account Management)</u>

(๑) ผู้ใช้งานทุกคนต้องมีบัญชีผู้ใช้งาน (User Account) เป็นของตนเองก่อนเข้าใช้งานระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือบริการดิจิทัลของมหาวิทยาลัย

(๒) การสร้าง แก้ไข ระงับ ยกเลิก หรือเพิกถอนบัญชีผู้ใช้งาน ต้องได้รับอนุมัติจากผู้มีอำนาจหรือผู้รับผิดชอบตามที่มหาวิทยาลัยกำหนด

(๓) บัญชีผู้ใช้งานต้องกำหนดให้สามารถระบุตัวตนของผู้ใช้งานได้อย่างชัดเจน และไม่อนุญาตให้ใช้บัญชีผู้ใช้งานร่วมกัน เว้นแต่เป็นบัญชีสำหรับงานระบบที่ได้รับอนุญาตโดยเฉพาะ

(๔) เมื่อผู้ใช้งานพ้นสภาพ เปลี่ยนตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดความจำเป็นในการใช้งาน ต้องดำเนินการปรับปรุง ระงับ หรือเพิกถอนบัญชีผู้ใช้งานโดยไม่ชักช้า

(๕) หน่วยงานที่รับผิดชอบต้องทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

<u>การกำหนดสิทธิการเข้าถึง (Access Control)</u>

(๑) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศต้องเป็นไปตามบทบาทหน้าที่ ความรับผิดชอบ และความจำเป็นในการปฏิบัติงาน

(๒) การกำหนดสิทธิการเข้าถึงต้องยึดหลักสิทธิเท่าที่จำเป็น (Least Privilege Principle) และหลักความจำเป็นต้องรู้ (Need-to-Know Principle)

(๓) ผู้ใช้งานต้องได้รับสิทธิเฉพาะที่จำเป็นต่อการปฏิบัติงานเท่านั้น และไม่ให้สิทธิที่เกินความจำเป็น

(๔) เจ้าของข้อมูล (Data Owner) หรือเจ้าของระบบ (System Owner) ต้องพิจารณาอนุมัติสิทธิการเข้าถึงตามอำนาจหน้าที่ที่กำหนด

(๕) ต้องมีการทบทวนสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ และอย่างน้อยปีละ ๑ ครั้ง

(๖) เมื่อผู้ใช้งานพ้นสภาพ เปลี่ยนตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดหน้าที่ความรับผิดชอบ ต้องมีการเพิกถอนหรือปรับปรุงสิทธิการเข้าถึงให้สอดคล้องกับสถานะปัจจุบันโดยไม่ชักช้า

การพิสูจน์ตัวตนและการยืนยันตัวตน (Authentication)

(๑) ผู้ใช้งานต้องผ่านกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบสารสนเทศหรือบริการดิจิทัลของมหาวิทยาลัย

(๒) ระบบที่มีความสำคัญ ระบบที่มีข้อมูลส่วนบุคคล ระบบที่มีข้อมูลลับ หรือระบบที่มีความเสี่ยงสูง ต้องใช้การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) หรือมาตรการอื่นที่มีระดับความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่า

(๓) ห้ามเปิดเผยข้อมูลที่ใช้ในการพิสูจน์ตัวตนแก่บุคคลอื่น

(๔) ผู้ใช้งานต้องแจ้งศูนย์เทคโนโลยีสารสนเทศ หรือหน่วยงานที่มหาวิทยาลัยกำหนดเมื่อพบหรือสงสัยว่าข้อมูลการพิสูจน์ตัวตนถูกเปิดเผย สูญหาย หรือถูกนำไปใช้โดยไม่ได้รับอนุญาต

(๕) การกำหนดข้อมูลสำหรับการพิสูจน์ตัวตนครั้งแรก และการรีเซ็ตรหัสผ่าน ต้องดำเนินการผ่านกระบวนการที่สามารถยืนยันตัวตนของผู้ขอใช้บริการได้อย่างเหมาะสม

การบริหารจัดการรหัสผ่าน (Password Management)

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีความเหมาะสมและมีความมั่นคงปลอดภัยทั้งนี้ หลักเกณฑ์เกี่ยวกับความยาว ความซับซ้อน อายุการใช้งาน และการเปลี่ยนรหัสผ่าน ให้เป็นไปตามมาตรฐานหรือข้อกำหนดที่มหาวิทยาลัยกำหนด

(๒) รหัสผ่านต้องไม่เป็นข้อมูลที่สามารถคาดเดาได้ง่าย เช่น ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขโทรศัพท์ หรือข้อมูลส่วนบุคคลอื่น

(๓) ห้ามเปิดเผย ส่งต่อ หรือแบ่งปันรหัสผ่านให้แก่บุคคลอื่น

(๔) กรณีสงสัยว่ารหัสผ่านอาจถูกเปิดเผย ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที

(๕) ผู้ดูแลระบบต้องมีมาตรการจัดเก็บและบริหารจัดการรหัสผ่านอย่างปลอดภัย

การควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ

(๑) การเข้าถึงระบบเครือข่าย ระบบสารสนเทศ และบริการดิจิทัลของมหาวิทยาลัย ต้องได้รับอนุญาตตามสิทธิที่กำหนด

(๒) ต้องมีมาตรการควบคุมการเข้าถึงระบบจากภายนอกมหาวิทยาลัยตามระดับความเสี่ยงของระบบ

(๓) การเข้าถึงระบบที่มีข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลลับ ต้องมีมาตรการควบคุมเพิ่มเติมตามความเหมาะสม

(๔) ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และติดตามตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับการเข้าถึงระบบ

(๕) การอนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศหรือระบบเครือข่ายของมหาวิทยาลัย ต้องได้รับอนุมัติจากผู้มีอำนาจ และต้องกำหนดขอบเขต ระยะเวลา และสิทธิการเข้าถึงอย่างชัดเจน

การบริหารจัดการบัญชีผู้ใช้งานสิทธิพิเศษ (Privileged Account Management)

(๑) บัญชีผู้ดูแลระบบหรือบัญชีที่มีสิทธิพิเศษต้องได้รับการควบคุมเป็นพิเศษ

(๒) การกำหนดสิทธิพิเศษต้องได้รับอนุมัติจากผู้มีอำนาจตามที่มหาวิทยาลัยกำหนด

(๓) ต้องจำกัดจำนวนผู้ที่มีสิทธิพิเศษเท่าที่จำเป็นต่อการปฏิบัติงาน

(๔) การใช้งานบัญชีสิทธิพิเศษต้องสามารถตรวจสอบย้อนหลังได้

(๕) ต้องมีการทบทวนบัญชีสิทธิพิเศษอย่างน้อยปีละ ๑ ครั้ง

การบันทึกและตรวจสอบการเข้าถึง (Access Logging and Monitoring)

(๑) ระบบสารสนเทศที่สำคัญต้องมีการบันทึกข้อมูลการเข้าใช้งานและเหตุการณ์ที่เกี่ยวข้องกับการเข้าถึงระบบ

(๒) บันทึกเหตุการณ์ (Log) ต้องได้รับการป้องกันจากการแก้ไข เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต

(๓) ศูนย์เทคโนโลยีสารสนเทศ หรือหน่วยงานที่มหาวิทยาลัยกำหนดต้องสามารถตรวจสอบและวิเคราะห์ข้อมูลการเข้าใช้งานเมื่อเกิดเหตุการณ์ผิดปกติหรือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(๔) การจัดเก็บบันทึกเหตุการณ์ต้องเป็นไปตามกฎหมาย ระเบียบ ข้อกำหนดที่เกี่ยวข้อง และต้องสามารถตรวจสอบย้อนหลังได้ตามระยะเวลาที่กฎหมายกำหนด

๖.๓ นโยบายการดูแลความปลอดภัยเชิงกายภาพ

วัตถุประสงค์

เพื่อป้องกันความเสียหาย การสูญหาย หรือการเข้าถึงทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาตจากภัยคุกคามทางกายภาพและสิ่งแวดล้อม

นโยบาย

มหาวิทยาลัยกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับอาคาร สถานที่ ห้องปฏิบัติการคอมพิวเตอร์ ศูนย์ข้อมูล อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และสื่อบันทึกข้อมูลเพื่อป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

<u>การกำหนดและควบคุมพื้นที่สำคัญ</u>

(๑) มหาวิทยาลัยต้องกำหนดพื้นที่ที่มีความสำคัญต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและการประมวลผลข้อมูลสารสนเทศ เช่น ศูนย์ข้อมูล ห้องแม่ข่าย ห้องควบคุมระบบ และพื้นที่จัดเก็บสื่อบันทึกข้อมูล

(๒) พื้นที่สำคัญต้องมีมาตรการควบคุมการเข้า-ออกที่เหมาะสมตามระดับความเสี่ยงของพื้นที่

(๓) บุคคลที่ไม่มีหน้าที่เกี่ยวข้องต้องไม่ได้รับอนุญาตให้เข้าถึงพื้นที่สำคัญ เว้นแต่ได้รับอนุญาตจากผู้รับผิดชอบ

(๔) ต้องมีการกำหนดผู้รับผิดชอบดูแลพื้นที่สำคัญอย่างชัดเจน

การควบคุมการเข้า-ออกพื้นที่ควบคุม

(๑) การเข้า-ออกพื้นที่ควบคุมต้องเป็นไปตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

(๒) มหาวิทยาลัยต้องกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ เช่น บัตรประจำตัว ระบบควบคุมการเข้า-ออก ระบบสแกนชีวมิติ หรือมาตรการอื่นที่เหมาะสมตามระดับความเสี่ยง

(๓) ต้องมีการบันทึกหรือสามารถตรวจสอบข้อมูลการเข้า-ออกพื้นที่ควบคุมได้ตามความเหมาะสม

(๔) กรณีบุคคลภายนอกเข้าพื้นที่ควบคุม ต้องได้รับอนุญาตและอยู่ภายใต้การกำกับดูแลของผู้รับผิดชอบ

การรักษาความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินสารสนเทศ

(๑) อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย สื่อบันทึกข้อมูล และทรัพย์สินสารสนเทศอื่น ต้องได้รับการป้องกันจากการสูญหาย การโจรกรรม ความเสียหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) การติดตั้ง เคลื่อนย้าย ซ่อมบำรุง หรือเปลี่ยนแปลงอุปกรณ์ ต้องได้รับอนุญาตจากผู้รับผิดชอบตามที่มหาวิทยาลัยกำหนด

(๓) อุปกรณ์ที่จัดเก็บข้อมูลสำคัญหรือข้อมูลส่วนบุคคลต้องมีมาตรการคุ้มครองเพิ่มเติมตามความเหมาะสม

(๔) อุปกรณ์หรือสื่อบันทึกข้อมูลที่หมดอายุการใช้งาน ชำรุด หรือยกเลิกการใช้งาน ต้องได้รับการลบทำลาย หรือกำจัดข้อมูลอย่างปลอดภัยก่อนจำหน่าย โอนย้าย หรือทำลายอุปกรณ์

การควบคุมสภาพแวดล้อมของพื้นที่สำคัญ

(๑) พื้นที่ที่ติดตั้งระบบสารสนเทศหรืออุปกรณ์สำคัญต้องมีสภาพแวดล้อมที่เหมาะสมต่อการทำงานของอุปกรณ์

(๒) ต้องมีมาตรการป้องกันความเสี่ยงจากอัคคีภัย น้ำท่วม ไฟฟ้าขัดข้อง ความร้อน ความชื้น หรือภัยคุกคามทางกายภาพอื่นที่อาจส่งผลกระทบต่อการดำเนินงาน

(๓) ระบบสาธารณูปโภคที่สนับสนุนการทำงานของระบบสารสนเทศต้องได้รับการตรวจสอบและบำรุงรักษาตามความเหมาะสม

การปฏิบัติตามหลักการโต๊ะทำงานสะอาด (Clear Desk Policy)

(๑) ผู้ใช้งานต้องไม่วางเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลที่มีข้อมูลสำคัญหรือข้อมูลลับไว้ในที่เปิดเผยโดยไม่มีผู้ดูแล

(๒) เมื่อเลิกใช้งานหรือออกจากพื้นที่ปฏิบัติงาน ต้องจัดเก็บเอกสารและสื่อบันทึกข้อมูลในสถานที่ที่เหมาะสมและปลอดภัย

(๓) เอกสารที่มีข้อมูลสำคัญหรือข้อมูลส่วนบุคคลต้องได้รับการจัดเก็บในพื้นที่ที่มีการควบคุมการเข้าถึง

การปฏิบัติเพื่อความปลอดภัยบนหน้าจอคอมพิวเตอร์ (Clear Screen Policy)

(๑) ผู้ใช้งานต้องล็อกหน้าจอหรือออกจากระบบเมื่อไม่อยู่ที่เครื่องคอมพิวเตอร์หรืออุปกรณ์สารสนเทศ

(๒) ต้องกำหนดให้ระบบสามารถล็อกหน้าจอโดยอัตโนมัติภายในระยะเวลาที่เหมาะสมเมื่อไม่มีการใช้งาน

(๓) ต้องหลีกเลี่ยงการแสดงข้อมูลสำคัญหรือข้อมูลลับในพื้นที่ที่บุคคลอื่นสามารถมองเห็นได้โดยไม่จำเป็น

การนำทรัพย์สินสารสนเทศออกนอกพื้นที่มหาวิทยาลัย

(๑) การนำอุปกรณ์คอมพิวเตอร์ สื่อบันทึกข้อมูล หรือทรัพย์สินสารสนเทศออกนอกพื้นที่มหาวิทยาลัยต้องได้รับอนุญาตจากผู้มีอำนาจหรือผู้รับผิดชอบตามที่กำหนด

(๒) ผู้ได้รับอนุญาตต้องรับผิดชอบในการดูแลรักษาทรัพย์สินสารสนเทศดังกล่าวตลอดระยะเวลาที่นำออกไปใช้งาน

(๓) กรณีทรัพย์สินสารสนเทศสูญหาย ถูกขโมย หรือได้รับความเสียหาย ต้องรายงานต่อหน่วยงานที่รับผิดชอบโดยทันที

(๔) กรณีพบเหตุการณ์ด้านความมั่นคงปลอดภัยทางกายภาพ หรือการเข้าถึงพื้นที่ควบคุมโดยไม่ได้รับอนุญาต ต้องรายงานต่องานศูนย์เทคโนโลยีสารสนเทศ หรือหน่วยงานที่มหาวิทยาลัยกำหนดโดยทันที

การจัดการผู้มาติดต่อและบุคคลภายนอก

(๑) บุคคลภายนอกที่เข้าปฏิบัติงานหรือเข้าพื้นที่ควบคุมของมหาวิทยาลัยต้องได้รับอนุญาตตามขั้นตอนที่กำหนด

(๒) บุคคลภายนอกต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของมหาวิทยาลัย

(๓) การเข้าถึงพื้นที่ที่มีข้อมูลสำคัญหรือระบบสำคัญต้องอยู่ภายใต้การกำกับดูแลของผู้รับผิดชอบตลอดระยะเวลาที่เข้าพื้นที่

(๔) การถ่ายภาพ บันทึกภาพ บันทึกเสียง หรือบันทึกข้อมูลภายในพื้นที่ควบคุม ต้องได้รับอนุญาตจากผู้รับผิดชอบตามที่มหาวิทยาลัยกำหนด และต้องไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ระบบสารสนเทศ หรือทรัพย์สินสารสนเทศของมหาวิทยาลัย

๖.๔ นโยบายการสำรองข้อมูลและการบริหารความต่อเนื่อง

วัตถุประสงค์

เพื่อให้มหาวิทยาลัยสามารถกู้คืนข้อมูลและระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสมเมื่อเกิดเหตุขัดข้องหรือสถานการณ์ฉุกเฉิน

นโยบาย

มหาวิทยาลัยกำหนดให้มีการสำรองข้อมูล การกู้คืนข้อมูล การกู้คืนระบบสารสนเทศ และการบริหารความต่อเนื่องทางธุรกิจอย่างเหมาะสม รวมทั้งมีการทดสอบแผนและทบทวนมาตรการเป็นระยะ เพื่อให้การดำเนินงานสามารถดำเนินต่อไปได้อย่างต่อเนื่อง

แนวปฏิบัติ

การสำรองข้อมูล (Backup Management)

(๑) ข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเทคโนโลยีสารสนเทศที่มีความสำคัญต่อการดำเนินงานของมหาวิทยาลัย ต้องได้รับการสำรองข้อมูลอย่างเหมาะสมตามระดับความสำคัญและความเสี่ยงของข้อมูลหรือระบบ

(๒) หน่วยงานเจ้าของข้อมูล (Data Owner) และเจ้าของระบบ (System Owner) ต้องกำหนดข้อมูลที่จำเป็นต้องสำรอง ความถี่ในการสำรองข้อมูล และระยะเวลาการเก็บรักษาข้อมูลสำรองให้เหมาะสม

(๓) การสำรองข้อมูลต้องครอบคลุมข้อมูล ระบบงาน การตั้งค่าระบบ และองค์ประกอบอื่นที่จำเป็นต่อการกู้คืนการให้บริการ

(๔) ต้องมีการติดตาม ตรวจสอบ และบันทึกผลการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการสำรองข้อมูลดำเนินการได้อย่างถูกต้องและครบถ้วน

การจัดเก็บและคุ้มครองข้อมูลสำรอง

(๑) ข้อมูลสำรองต้องได้รับการจัดเก็บในสถานที่หรือระบบที่มีความมั่นคงปลอดภัย และได้รับการคุ้มครองตามระดับชั้นความลับของข้อมูล

(๒) การจัดเก็บข้อมูลสำรองต้องดำเนินการในรูปแบบที่เหมาะสมกับระดับความสำคัญและความเสี่ยงของข้อมูล โดยอาจจัดเก็บในสื่อบันทึกข้อมูล ระบบจัดเก็บข้อมูลสำรอง ศูนย์ข้อมูลสำรอง หรือบริการคลาวด์ที่ได้รับอนุญาตจากมหาวิทยาลัย

(๓) ต้องมีมาตรการป้องกันการเข้าถึง การเปลี่ยนแปลง การเปิดเผย หรือการทำลายข้อมูลสำรองโดยไม่ได้รับอนุญาต

(๔) การเข้าถึงข้อมูลสำรองต้องจำกัดเฉพาะผู้ที่ได้รับมอบหมายหรือได้รับอนุญาตเท่านั้น

การกู้คืนข้อมูลและการกู้คืนระบบสารสนเทศ

(๑) มหาวิทยาลัยต้องมีมาตรการและขั้นตอนในการกู้คืนข้อมูลและกู้คืนระบบสารสนเทศเมื่อเกิดเหตุขัดข้อง เหตุฉุกเฉิน หรือเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการ

(๒) หน่วยงานที่รับผิดชอบต้องกำหนดลำดับความสำคัญของระบบและข้อมูลที่ต้องได้รับการกู้คืนเพื่อให้สามารถกลับมาให้บริการได้ภายในระยะเวลาที่เจ้าของระบบ (System Owner) หรือมหาวิทยาลัยกำหนดตามระดับความสำคัญของระบบและข้อมูล

(๓) การกู้คืนข้อมูลและระบบสารสนเทศต้องคำนึงถึงความถูกต้องครบถ้วน ความพร้อมใช้งาน และความมั่นคงปลอดภัยของข้อมูล

(๔) ต้องมีการจัดทำและปรับปรุงเอกสารขั้นตอนการกู้คืนข้อมูลและระบบสารสนเทศให้เป็นปัจจุบันอยู่เสมอ

(๕) เจ้าของระบบ (System Owner) ต้องกำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และเป้าหมายจุดกู้คืนข้อมูล (Recovery Point Objective: RPO) ตามระดับความสำคัญและความเสี่ยงของระบบหรือข้อมูลตามที่มหาวิทยาลัยกำหนด

การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

(๑) มหาวิทยาลัยต้องกำหนดมาตรการรองรับเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานของระบบสารสนเทศและบริการดิจิทัล เพื่อให้สามารถดำเนินภารกิจสำคัญได้อย่างต่อเนื่อง

(๒) หน่วยงานที่เกี่ยวข้องต้องจัดทำและทบทวนแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan: DRP) ตามความเหมาะสม และต้องปรับปรุงเมื่อมีการเปลี่ยนแปลงระบบ กระบวนการ หรือความเสี่ยงที่มีนัยสำคัญ

(๓) แผนบริหารความต่อเนื่องต้องครอบคลุมบทบาทหน้าที่ของผู้เกี่ยวข้อง ช่องทางการสื่อสาร การบริหารจัดการทรัพยากร และแนวทางการดำเนินงานในภาวะฉุกเฉิน

(๔) ต้องมีการกำหนดผู้รับผิดชอบในการดำเนินงานตามแผนและการประสานงานเมื่อเกิดเหตุการณ์ฉุกเฉิน

<u>การทดสอบและทบทวนแผน</u>

(๑) มหาวิทยาลัยต้องดำเนินการทดสอบการสำรองข้อมูล การกู้คืนข้อมูล และการกู้คืนระบบสารสนเทศเป็นระยะตามความเหมาะสม และต้องมีการบันทึกผลการทดสอบ รวมถึงผลการกู้คืนที่สามารถพิสูจน์ได้ว่าข้อมูลและระบบสามารถกลับมาใช้งานได้จริง

(๒) ต้องมีการทดสอบแผนบริหารความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(๓) ผลการทดสอบต้องได้รับการบันทึก ประเมินผล และนำไปใช้ในการปรับปรุงมาตรการ แผนงาน หรือขั้นตอนการดำเนินงานให้มีประสิทธิภาพยิ่งขึ้น

(๔) หน่วยงานที่เกี่ยวข้องต้องทบทวนความเหมาะสมของแผนและมาตรการด้านการสำรองข้อมูลและการบริหารความต่อเนื่องอย่างสม่ำเสมอ

<u>การรายงานและการปรับปรุง</u>

(๑) กรณีพบปัญหา ความผิดปกติ หรือข้อบกพร่องที่อาจส่งผลกระทบต่อการสำรองข้อมูล การกู้คืนข้อมูล หรือการดำเนินงานตามแผนบริหารความต่อเนื่อง ต้องรายงานต่องานศูนย์เทคโนโลยีสารสนเทศ หรือหน่วยงานที่มหาวิทยาลัยกำหนดโดยทันที และดำเนินการตามนโยบายการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย

(๒) หน่วยงานที่เกี่ยวข้องต้องดำเนินการวิเคราะห์สาเหตุ ปรับปรุงมาตรการ และติดตามผลการแก้ไขเพื่อป้องกันการเกิดเหตุซ้ำ

(๓) ผลการทดสอบ การทบทวน และการปรับปรุงแผน ต้องจัดเก็บเป็นหลักฐานเพื่อใช้ในการตรวจสอบและประเมินผลตามที่มหาวิทยาลัยกำหนด

<u>การกำหนดบทบาทและความรับผิดชอบ</u>

(๑) เจ้าของข้อมูล (Data Owner) เจ้าของระบบ (System Owner) ผู้ดูแลระบบ และหน่วยงานที่เกี่ยวข้อง ต้องมีบทบาทและความรับผิดชอบด้านการสำรองข้อมูล การกู้คืนข้อมูล และการบริหารความต่อเนื่องตามที่มหาวิทยาลัยกำหนด

(๒) ต้องมีการกำหนดผู้รับผิดชอบหลักและผู้ปฏิบัติสำรองสำหรับกระบวนการสำคัญที่เกี่ยวข้องกับการกู้คืนระบบและการดำเนินงานในภาวะฉุกเฉิน

๖.๕ นโยบายการรายงานเหตุการณ์ละเมิดและความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อให้มหาวิทยาลัยสามารถตรวจพบ รายงาน ตอบสนอง และจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างรวดเร็วและมีประสิทธิภาพ

นโยบาย

มหาวิทยาลัยกำหนดให้มีการเฝ้าระวัง ตรวจสอบ รายงาน บันทึก วิเคราะห์ ตอบสนอง และติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เหตุการณ์ทางไซเบอร์ และเหตุละเมิดข้อมูลส่วนบุคคล รวมทั้งจัดเก็บหลักฐานและรายงานต่อหน่วยงานที่เกี่ยวข้องตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

แนวปฏิบัติ

<u>การเฝ้าระวังและตรวจพบเหตุการณ์</u>

(๑) มหาวิทยาลัยต้องมีมาตรการเฝ้าระวัง ตรวจสอบ และติดตามเหตุการณ์ที่อาจส่งผลกระทบต่อข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ หรือทรัพย์สินสารสนเทศของมหาวิทยาลัย

(๒) ผู้ดูแลระบบและหน่วยงานที่เกี่ยวข้องต้องติดตามข้อมูลบันทึกเหตุการณ์ (Log) สัญญาณเตือน และข้อมูลอื่นที่เกี่ยวข้อง เพื่อใช้ในการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(๓) ผู้ใช้งานทุกคนมีหน้าที่สังเกตและแจ้งเหตุเมื่อพบความผิดปกติหรือเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

<u>การรายงานเหตุการณ์</u>

(๑) เมื่อพบหรือสงสัยว่าเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เหตุการณ์ทางไซเบอร์ หรือเหตุละเมิดข้อมูลส่วนบุคคล ผู้ใช้งานต้องรายงานต่องานศูนย์เทคโนโลยีสารสนเทศ หรือหน่วยงานที่มหาวิทยาลัยกำหนดโดยทันที

(๒) การรายงานเหตุการณ์ต้องระบุรายละเอียดที่จำเป็น เช่น วันเวลา ลักษณะเหตุการณ์ ระบบหรือข้อมูลที่ได้รับผลกระทบ และข้อมูลอื่นที่เกี่ยวข้องเท่าที่สามารถดำเนินการได้

(๓) ผู้รับแจ้งเหตุต้องดำเนินการบันทึกข้อมูลเหตุการณ์และประสานงานกับหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า

<u>การตอบสนองและจัดการเหตุการณ์</u>

(๑) หน่วยงานที่รับผิดชอบต้องประเมินระดับความรุนแรง ผลกระทบ และความเร่งด่วนของเหตุการณ์เพื่อกำหนดแนวทางตอบสนองที่เหมาะสม

(๒) ต้องดำเนินมาตรการควบคุมหรือจำกัดผลกระทบของเหตุการณ์โดยเร็วที่สุด เพื่อป้องกันความเสียหายที่อาจขยายวงกว้าง

(๓) การดำเนินการแก้ไข ฟื้นฟู หรือกู้คืนระบบต้องเป็นไปตามขั้นตอนที่กำหนด และต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ และอาจดำเนินการตามแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) หรือแผนกู้คืนระบบสารสนเทศ (DRP) ตามความเหมาะสมของเหตุการณ์

(๔) กรณีเหตุการณ์มีผลกระทบต่อข้อมูลส่วนบุคคล ให้ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและข้อกำหนดที่เกี่ยวข้อง

(๕) หน่วยงานที่รับผิดชอบต้องกำหนดหลักเกณฑ์การจัดระดับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศตามระดับความรุนแรง ผลกระทบ และความเร่งด่วน เพื่อใช้ในการตอบสนองและบริหารจัดการเหตุการณ์อย่างเหมาะสม

<u>การเก็บรักษาพยานหลักฐานและข้อมูลที่เกี่ยวข้อง</u>

(๑) หน่วยงานที่รับผิดชอบต้องดำเนินการเก็บรักษาพยานหลักฐาน ข้อมูลบันทึกเหตุการณ์ (Log) และข้อมูลที่เกี่ยวข้องกับเหตุการณ์อย่างเหมาะสม

(๒) การเก็บรักษาพยานหลักฐานต้องดำเนินการในลักษณะที่ไม่ส่งผลกระทบต่อความถูกต้องครบถ้วนและความน่าเชื่อถือของข้อมูล

(๓) การเข้าถึงพยานหลักฐานและข้อมูลที่เกี่ยวข้องกับเหตุการณ์ต้องจำกัดเฉพาะผู้มีหน้าที่รับผิดชอบหรือผู้ได้รับอนุญาต

(๔) การเก็บรักษา การส่งมอบ หรือการเข้าถึงพยานหลักฐาน ต้องสามารถตรวจสอบผู้ครอบครอง ผู้ดำเนินการ และช่วงเวลาที่เกี่ยวข้องได้ เพื่อรักษาความน่าเชื่อถือของพยานหลักฐาน

<u>การแจ้งเตือนและการรายงานต่อหน่วยงานที่เกี่ยวข้อง</u>

(๑) กรณีเหตุการณ์มีผลกระทบในระดับที่กฎหมายกำหนด หรือมีผลกระทบต่อบุคคล หน่วยงาน หรือผู้มีส่วนได้ส่วนเสีย มหาวิทยาลัยต้องดำเนินการแจ้งเตือนหรือรายงานต่อหน่วยงานที่เกี่ยวข้องตามกฎหมาย ระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง

(๒) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต้องดำเนินการตามหลักเกณฑ์และระยะเวลาที่กฎหมายกำหนด

(๓) การสื่อสารข้อมูลเกี่ยวกับเหตุการณ์ต่อสาธารณะหรือสื่อมวลชนให้เป็นอำนาจของผู้บริหารหรือผู้ที่ได้รับมอบหมายจากมหาวิทยาลัยเท่านั้น

(๔) กรณีเป็นเหตุการณ์ที่มีผลกระทบในระดับร้ายแรงหรืออาจส่งผลกระทบในวงกว้าง มหาวิทยาลัยต้องรายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการที่เกี่ยวข้องตามกระบวนการที่มหาวิทยาลัยกำหนด

<u>การบันทึกและติดตามผล</u>

(๑) เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศทุกกรณีต้องได้รับการบันทึกและจัดเก็บข้อมูลตามรูปแบบที่มหาวิทยาลัยกำหนด

(๒) ต้องมีการติดตามผลการดำเนินงานจนกว่าเหตุการณ์จะได้รับการแก้ไขหรือปิดเหตุการณ์อย่างเป็นทางการ

(๓) เอกสาร บันทึก และหลักฐานที่เกี่ยวข้องกับเหตุการณ์ต้องได้รับการจัดเก็บเพื่อใช้ในการตรวจสอบและประเมินผลในอนาคต

<u>การทบทวนและปรับปรุงมาตรการ</u>

(๑) ภายหลังการจัดการเหตุการณ์ หน่วยงานที่เกี่ยวข้องต้องดำเนินการวิเคราะห์สาเหตุ ผลกระทบ และบทเรียนที่ได้รับจากเหตุการณ์

(๒) ต้องกำหนดมาตรการป้องกัน แก้ไข หรือปรับปรุงกระบวนการทำงานเพื่อป้องกันการเกิดเหตุซ้ำ

(๓) ผลการวิเคราะห์และข้อเสนอแนะในการปรับปรุงต้องได้รับการรายงานต่อผู้บริหารหรือผู้มีอำนาจตามที่มหาวิทยาลัยกำหนด

(๔) มหาวิทยาลัยต้องทบทวนและปรับปรุงมาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง โดยคำนึงถึงผลการดำเนินงาน เหตุการณ์ที่เกิดขึ้น และความเสี่ยงที่เปลี่ยนแปลงไป

(๕) หน่วยงานที่เกี่ยวข้องควรจัดให้มีการทบทวนหลังเหตุการณ์ (Post-Incident Review) เพื่อสรุปบทเรียน ปัญหา อุปสรรค และแนวทางปรับปรุงมาตรการด้านความมั่นคงปลอดภัยสารสนเทศในอนาคต

ข้อมูลเอกสาร

ชื่อเอกสาร	คู่มือนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
Document Title	Information Security Policy and Guidelines
รหัสเอกสาร	IT-SEC-GDL-๒๕๖๙
สถานะเอกสาร	ใช้งาน (Effective)

เอกสารฉบับนี้เป็นเอกสารควบคุมของมหาวิทยาลัย (Controlled Document) การแก้ไขเปลี่ยนแปลงต้องได้รับการอนุมัติตามกระบวนการที่มหาวิทยาลัยกำหนด

ประวัติเอกสาร

รุ่นเอกสาร	วันที่อนุมัติ/เริ่มใช้งานเอกสาร	ผู้อนุมัติ	สาระสำคัญที่แก้ไข
Ver.๑	๒๕๖๙	อธิการบดี	จัดทำเอกสารฉบับแรก

ผู้รับผิดชอบการดำเนินการ

การดำเนินการ	ผู้รับผิดชอบ
การประกาศใช้	อธิการบดี
การจัดทำเอกสาร	ศูนย์เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
การทบทวนเอกสาร	ศูนย์เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และเสนออธิการบดีพิจารณา

การเผยแพร่

ช่องทาง	รายละเอียด
เว็บไซต์	
หนังสือเวียน	
เอกสารเผยแพร	
อื่น ๆ	

เอกสารที่เกี่ยวข้อง

เอกสาร	ชื่อเอกสาร
เอกสารภายใน	ประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
เอกสารภายนอก	พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทาง อิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ประวัติการทบทวน

รหัสเอกสาร	ผู้จัดทำ/ผู้ทบทวน	รายละเอียด
IT-SEC-POL-๒๕๖๙ (Ver.๑)	ISDP	-

ผู้อนุมัติ (Approved by): อธิการบดีมหาวิทยาลัยราชภัฏรำไพพรรณี
ผู้รับผิดชอบเอกสาร (Document Custodian): สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
หน่วยงานรับผิดชอบ: สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ระดับเอกสาร: ใช้ภายในองค์กร (Internal Use Only) และถือเป็นเอกสารแนบท้ายประกาศมหาวิทยาลัยราชภัฏรำไพพรรณี เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๙
รอบการทบทวน: อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

ประวัติการแก้ไขเอกสาร (Revision History)

รุ่นเอกสาร	วันที่อนุมัติ	ผู้อนุมัติ	สาระสำคัญที่แก้ไข	ผู้จัดทำ/ผู้แก้ไข
๑.๐	๑๗ มิถุนายน ๒๕๖๙	อธิการบดี	จัดทำเอกสารฉบับแรก	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ