ประกาศมหาวิทยาลัยราชภัฏจันทรเกษม
เรื่อง มาตรการรักษาความมั่นคงปลอดภัย การเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคล

มหาวิทยาลัยราชภัฏจันทรเกษม ซึ่งต่อไปนี้จะเรียกว่า “มหาวิทยาลัย” ตระหนักและให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนั้น เพื่อให้เกิดความมั่นใจว่าข้อมูลส่วนบุคคลจะได้รับความคุ้มครองตามกฎหมาย มหาวิทยาลัยจึงได้จัดทำมาตรการเพื่อกำหนดรายละเอียดในการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย รวมทั้งการจัดเก็บ และการทำลายข้อมูลส่วนบุคคลของมหาวิทยาลัยราชภัฏจันทรเกษม ดังนี้

๑. มาตรการรักษาความมั่นคงปลอดภัย

(๑) มาตรการเชิงองค์กร

(๑.๑) มหาวิทยาลัยจะดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในระดับที่เหมาะสม เพื่อป้องกันการสูญหายของข้อมูล การเข้าถึงโดยไม่ได้รับอนุญาต และการละเมิดข้อมูลส่วนบุคคลโดยดำเนินการแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้แก่ ผู้บริหาร และบุคลากรทุกระดับของมหาวิทยาลัย รวมทั้งสร้างเสริมความตระหนักรู้เพื่อให้เห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่นำมาใช้ในการประมวลผลต่าง ๆ

(๑.๒) มหาวิทยาลัยจะดำเนินการระบุความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ การป้องกันความเสี่ยงที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล โดยเป็นไปตามนโยบายการรักษาความปลอดภัยทางสารสนเทศ กำหนดหน้าที่ความรับผิดชอบให้แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยในการดำเนินการเมื่อเกิดเหตุละเมิด และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล

(๑.๓) มหาวิทยาลัยมีการบริหารจัดการการเข้าถึงของผู้ใช้งาน โดยกำหนดสิทธิและอนุญาตเฉพาะรายในการเข้าถึงข้อมูลส่วนบุคคล เช่น สิทธิในการเข้าถึงข้อมูล แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบข้อมูล ตลอดจนการลบและทำลาย

(๒) มาตรการเชิงเทคนิค

มหาวิทยาลัยได้นำเทคโนโลยีและมาตรฐานที่เหมาะสมในการปกป้องข้อมูลส่วนบุคคลมาใช้ในการดำเนินงานของมหาวิทยาลัย ได้แก่

(๒.๑) การเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒.๒) การควบคุมสิทธิเข้าถึงข้อมูล (Access Control) โดยใช้ระบบรหัสผ่านหรือการยืนยันตัวตนสองขั้นตอน (๒FA)

(๒.๓) การตรวจสอบและบันทึกกิจกรรมของระบบ (Logging & Monitoring) เพื่อป้องกันและตรวจสอบเหตุการณ์ผิดปกติ

(๒.๔) การทำลายข้อมูลในอุปกรณ์จัดเก็บข้อมูล

(๓) มาตรการทางกายภาพ

(๓.๑) มหาวิทยาลัยมีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น บุคลากรผู้รับผิดชอบพื้นที่ในการจัดเก็บข้อมูลส่วนบุคคล ทั้งข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Digital Data) และข้อมูลในรูปแบบเอกสาร (Physical Data) มาตรการตรวจสอบการเข้าออกอาคารหรือห้องเซิร์ฟเวอร์ (CCTV และระบบคีย์การ์ด) ตู้เก็บรักษาเอกสารข้อมูลส่วนบุคคล การจำกัดการเข้าถึงศูนย์ข้อมูล (Data Center) และพื้นที่จัดเก็บข้อมูลสำคัญ ระบบสำรองไฟ (UPS) และแผนการกู้คืนระบบ (Disaster Recovery Plan) เป็นต้น

(๓.๒) การบริหารจัดการและกำหนดสิทธิผู้ที่ได้รับอนุญาตให้เข้าถึงอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล ตามหน้าที่ความรับผิดชอบเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(๔) ข้อตกลงระหว่างมหาวิทยาลัยและผู้ประมวลผลข้อมูลส่วนบุคคล

กรณีมหาวิทยาลัยได้มอบหมายให้บุคคลหรือนิติบุคคลอื่นเป็นผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์แก่การดำเนินภารกิจของมหาวิทยาลัย มหาวิทยาลัยจะกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเทียบเท่าหรือดีกว่ามาตรการของมหาวิทยาลัยนี้ เพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ หรือกระทำโดยปราศจากอำนาจโดยชอบด้วยกฎหมาย รวมทั้งต้องมีการแจ้งให้มหาวิทยาลัยทราบโดยทันทีถ้าเกิดการละเมิดข้อมูลส่วนบุคคล

๒. การเก็บรักษาข้อมูลส่วนบุคคล

มหาวิทยาลัยจะดำเนินการเก็บรักษา รวมทั้งระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล ทั้งข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Digital Data) และข้อมูลในรูปแบบเอกสาร (Physical Data) ให้สอดคล้องกับวัตถุประสงค์ที่ได้กำหนดไว้ และอยู่ภายใต้ระยะเวลาตามประกาศความเป็นส่วนตัว (Privacy Notice) หรือบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities) แต่ละประเภท อนึ่ง หากหมดความจำเป็นหรือสิ้นสุดการใช้งานของข้อมูลส่วนบุคคล มหาวิทยาลัยจะดำเนินการลบหรือทำลายตามขั้นตอนต่อไป แต่อย่างไรก็ตาม หากไม่สามารถลบหรือทำลายข้อมูลส่วนบุคคลดังกล่าวได้ เพื่อนำไปใช้ในเชิงสถิติจะดำเนินการแปลงข้อมูลให้เป็นข้อมูลนิรนามก่อนนำไปประมวลผล

๓. การลบหรือทำลายข้อมูลส่วนบุคคล

(๑) แนวทางการลบหรือทำลายข้อมูลส่วนบุคคล

มหาวิทยาลัยจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูล หรือเกินความจำเป็นตามวัตถุประสงค์ หรือเจ้าของข้อมูลส่วนบุคคลร้องขอให้มีการลบหรือทำลายข้อมูลส่วนบุคคล ตามขั้นตอนดังนี้

(๑.๑) คณะกรรมการดำเนินงานขออนุญาตทำลายข้อมูลส่วนบุคคลที่ครบกำหนดระยะเวลาการเก็บรักษาหรือเจ้าของข้อมูลส่วนบุคคลมีการร้องขอเป็นหนังสือพร้อมระบุเหตุผลให้ลบหรือทำลายข้อมูลส่วนบุคคล

(๑.๒) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยพิจารณาและอนุมัติในการทำลายข้อมูลส่วนบุคคล ตามความจำเป็นแก่กรณี

(๑.๓) คณะกรรมการดำเนินงานบันทึกหลักฐานการทำลายข้อมูลส่วนบุคคล และรายงานให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยทราบ

(๒) วิธีการลบหรือทำลายข้อมูลส่วนบุคคล

(๒.๑) การลบข้อมูลจากฐานข้อมูล โดยใช้วิธี Secure Deletion หรือ Overwriting เพื่อให้มั่นใจว่าข้อมูลไม่สามารถกู้คืนได้ และตรวจสอบการลบข้อมูลผ่านบันทึกการทำงานของระบบ (Logs)

(๒.๒) การลบข้อมูลจากอีเมลและระบบคลาวด์ โดยใช้วิธีลบข้อมูลจาก ผู้ดูแลระบบอีเมล (admin control) และตรวจสอบว่าข้อมูลถูกลบอย่างถาวร - หากใช้บริการคลาวด์ (Google Drive, OneDrive) ให้ลบข้อมูลผ่านระบบผู้ดูแล (Admin Console)

(๒.๓) การทำลายข้อมูลในอุปกรณ์จัดเก็บข้อมูล โดยใช้ซอฟต์แวร์ลบข้อมูลที่ได้มาตรฐาน เช่น DBAN, CCleaner, Eraser หรือกรณีอุปกรณ์ที่ไม่ได้ใช้งานจะทำลายฮาร์ดไดรฟ์ด้วยเครื่องบด (Shredding)

กรณีข้อมูลในรูปแบบเอกสาร (Physical Data) จะใช้วิธีทำลาย เช่น Shredding (ย่อยเอกสาร), Burning (เผา), Pulping (บดเป็นเยื่อกระดาษ) เพื่อให้ไม่สามารถนำกลับมาใช้ได้

(๒.๔) การจัดทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Anonymization) ได้แก่

(๒.๔.๑) การผสมข้อมูล (Scrambling) เป็นการสลับลำดับของตัวอักษรในข้อมูลด้วยกฎเกณฑ์หนึ่ง ๆ เช่น ๐๑๒๓๔๕ แสดงเป็น ๒๑๐๓๔๕

(๒.๔.๒) การปิดทับข้อมูล (Masking) เป็นการเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูล เช่น ข้อมูลหมายเลขโทรศัพท์ ๐๙๘๗๖๕๔๓๒๑ แสดงเป็น ######๔๓๒๑

(๒.๔.๓) การลดความชัดเจนของข้อมูลลง (Blurring or Noising) เป็นการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง เช่น มีชุดข้อมูลเป็นสีรถและทะเบียนรถ อาจจะลดข้อมูลเหลือเพียงแค่สีรถ

(๒.๔.๔) การแฝงข้อมูล (Pseudonymization) เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูล โดยตรง เช่น ชื่อ ที่อยู่ และรหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมา

(๒.๔.๕) การจัดทำข้อมูลให้ระบุตัวตนไม่ได้ (De-identification) เป็นการลบข้อมูลในส่วนที่สามารถระบุตัวตน เพื่อป้องกันไม่ให้ระบุเชื่อมโยงข้อมูล หรือป้องกันการย้อนรอย เพื่อระบุตัวตน (Re-identification) กลับไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้องได้ เช่น มีชุดข้อมูล ชื่อ นายสมชาย ดวงดี somchai@example.com เบอร์โทร ๐๙๑๒๓๔๕๖๗๘ แสดงเป็น นาย A อีเมล – เบอร์โทร

๔. การตรวจสอบและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มหาวิทยาลัยจะดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัย การเก็บรักษาและการลบหรือทำลายข้อมูลส่วนบุคคลเป็นระยะ อย่างน้อยปีละ ๑ ครั้ง และจะปรับปรุงให้สอดคล้องกับการป้องกันภัยคุกคามทางไซเบอร์ รวมทั้งเทคโนโลยีที่เปลี่ยนแปลงไป

ประกาศ ณ วันที่ ๙ ตุลาคม พ.ศ. ๒๕๖๘

(นายสงกรานต์ สุขเกษม)
รองอธิการบดี ฝ่ายวิชาการ
ผู้บริหารคุ้มครองข้อมูลส่วนบุคคล