ประกาศมหาวิทยาลัยอัสสัมชัญ

ที่ ๑๓/๒๕๖๖

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖

โดยที่เห็นเป็นการสมควร เพื่อให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของมหาวิทยาลัยดำเนินไปอย่างมีประสิทธิภาพ อธิการบดีอาศัยอำนาจตามความในมาตรา ๔๓ แห่งพระราชบัญญัติสถาบันอุดมศึกษาเอกชน พ.ศ. ๒๕๔๖ แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๐ จึงกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของมหาวิทยาลัยอัสสัมชัญ ไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศมหาวิทยาลัยอัสสัมชัญ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖”

ข้อ ๒ วัตถุประสงค์ของประกาศนี้

๒.๑ เพื่อกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของมหาวิทยาลัยอัสสัมชัญ ให้ครอบคลุมด้านการบริหารจัดการ ด้านเทคนิค และด้านกายภาพ ในเรื่องการเข้าถึงหรือการควบคุมการใช้งานข้อมูลส่วนบุคคล

๒.๒ เพื่อให้ผู้มีส่วนเกี่ยวข้องใช้เป็นหลักปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย

๒.๓ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวของเจ้าของข้อมูลได้รับการปฏิบัติอย่างมีมาตรฐานและครอบคลุมการดำเนินงานของมหาวิทยาลัยอย่างครบถ้วน

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย”	หมายความว่า	มหาวิทยาลัยอัสสัมชัญ
“อธิการบดี”	หมายความว่า	อธิการบดีมหาวิทยาลัยอัสสัมชัญ
“หน่วยงาน”	หมายความว่า	คณะ สำนัก สาขา/ภาควิชา ศูนย์ สำนักงาน
“นโยบาย”	หมายความว่า	นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ในประกาศมหาวิทยาลัย
“ข้อมูลส่วนบุคคล”	หมายความว่า	ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อมแต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ
“การประมวลผลข้อมูลส่วนบุคคล”	หมายความว่า	การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือการดำเนินการ หรือชุดการดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลไม่ว่าจะโดยอัตโนมัติหรือไม่ เช่น การบันทึก จัดระบบ จัดโครงสร้าง เก็บรักษาเปลี่ยนแปลงหรือปรับเปลี่ยน การรับ การใช้ หรือเปิดเผยด้วยการส่งต่อเผยแพร่การกระทำอื่นใดเพื่อให้เกิดความพร้อมใช้งานการจัดวาง หรือผสมเข้าด้วยกัน การกำจัด ลบ หรือทำลายข้อมูลส่วนบุคคล

ต่อหน้าที่ ๒ / “ผู้ควบคุม...

"ผู้ควบคุมข้อมูลส่วนบุคคล"	หมายความว่า	รองอธิการบดี คณบดี นายทะเบียน ผู้อำนวยการ ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในหน่วยงานของตน
"ผู้ประมวลผลข้อมูลส่วนบุคคล"	หมายความว่า	บุคลากรของมหาวิทยาลัยผู้ได้รับมอบหมายจากผู้ควบคุมข้อมูลให้ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคล
"เจ้าของข้อมูล"	หมายความว่า	นักศึกษา บุคลากร ศิษย์เก่า บุคคลทั่วไป รวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ
"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล"	หมายความว่า	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่มหาวิทยาลัยแต่งตั้ง

ข้อ ๔ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

๔.๑ มหาวิทยาลัยมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสอดคล้องกับบทบัญญัติของกฎหมาย และมาตรฐานอื่นที่จำเป็น ทั้งนี้เพื่อรักษาสถานภาพด้านความลับ (Confidentiality) ด้านความถูกต้องสมบูรณ์ (Integrity) และด้านความพร้อมใช้งาน (Availability) โดยครอบคลุมการดำเนินการรักษาความมั่นคงปลอดภัย ดังนี้

๔.๑.๑ มาตรการป้องกันด้านการบริหารจัดการ

(๑) การป้องกันบุคคลที่มิได้รับอนุญาตให้ประมวลผลข้อมูลส่วนบุคคลเข้าถึงระบบการประมวลผลข้อมูลส่วนบุคคล เช่น การระบุผู้ได้รับอนุญาตให้เข้าถึงระบบประมวลผลข้อมูลส่วนบุคคลโดย Active Directory การกำหนดนโยบายเกี่ยวกับการใช้รหัสและการเปลี่ยนแปลงรหัสในการเข้าถึงข้อมูลส่วนบุคคล การกำหนดสิทธิเฉพาะบุคคลให้บุคลากรของมหาวิทยาลัย หรือผู้เชี่ยวชาญจากภายนอกที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการเข้าถึง บริหารจัดการ และบำรุงรักษาศูนย์กลางข้อมูลหรือระบบเครือข่ายเทคโนโลยีสารสนเทศ

(๒) การจำกัดการเข้าถึงข้อมูลส่วนบุคคลไว้ให้เฉพาะผู้ประมวลผลข้อมูลส่วนบุคคลที่มีความจำเป็นต้องใช้ข้อมูลในการปฏิบัติงานในหน้าที่แต่ละระดับชั้น และจัดให้มีการบันทึกและทำสำรองข้อมูลของการเข้าถึง หรือการเข้าใช้งานในระยะเวลาที่เหมาะสม หรือตามระยะเวลาที่กฎหมายกำหนด

(๓) การควบคุมมิให้บุคคลที่ได้รับอนุญาตให้เข้าถึงและประมวลผลข้อมูลส่วนบุคคลกระทำการเกินสิทธิและหน้าที่ที่ได้รับอนุญาต

(๔) การตรวจสอบย้อนกลับหากพบว่าข้อมูลส่วนบุคคลของบุคคลใดถูกเข้าถึง แก้ไข นำออกจากระบบ หรือถูกลบ

(๕) การควบคุมการปฏิบัติตามคำสั่งซึ่งสามารถรับรองได้ว่าการประมวลผลข้อมูลส่วนบุคคลจะเป็นไปตามข้อกำหนดหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล เช่น กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถแก้ไข ย้าย หรือลบข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับคำสั่งโดยเฉพาะเจาะจงจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น หรือกำหนดให้เมื่อผู้ประมวลผลข้อมูลส่วนบุคคลได้รับคำสั่งเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องกำหนดขั้นตอนหรือวิธีการเพื่อให้แน่ใจว่าการประมวลผลนั้นสอดคล้องกับข้อกำหนดด้านการตรวจสอบย้อนกลับ เป็นต้น

ต่อหน้าที่ ๓ / (๖) การควบคุม...

(๖) การควบคุมการแยกส่วนของข้อมูล โดยข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมด้วยวัตถุประสงค์ที่แตกต่างกันจะต้องดำเนินการประมวลผลแยกออกจากกัน

(๗) จัดให้มีระบบและกลไกการสื่อสารที่มีประสิทธิภาพ ทันต่อสถานการณ์ระหว่างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และบุคลากรอื่นที่เกี่ยวข้อง

(๘) จัดให้มีแผนบริหารความต่อเนื่องของกิจการ (Business Continuity Plan) โดยระบุวิธีการคุ้มครองป้องกันและกู้คืนข้อมูลส่วนบุคคลเอาไว้ในแผนดังกล่าวด้วย

(๙) จัดให้มีการทบทวนสิทธิการเข้าถึงข้อมูลส่วนบุคคลอยู่เสมอ หรืออย่างน้อยปีละ ๑ ครั้ง และเมื่อสิ้นสุดความจำเป็นที่ผู้รับผิดชอบข้อมูลส่วนบุคคลและผู้ปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลจะต้องใช้งานข้อมูล การโยกย้ายบุคลากร หรือการสิ้นสุดสัญญาจ้างบุคลากร ให้ยกเลิกสิทธิการเข้าถึงข้อมูลทันที

(๑๐) จัดให้มีการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นระยะ เพื่อให้เกิดความมั่นใจว่ามาตรการที่ใช้อยู่นั้นมีความเหมาะสมและมีประสิทธิภาพ

(๑๑) จัดทำและเผยแพร่มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลให้บุคลากรของมหาวิทยาลัยและบุคคลที่เกี่ยวข้องทราบ ตลอดจนส่งเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการและแนวปฏิบัติที่กำหนดอย่างเคร่งครัด

๔.๑.๒ มาตรการป้องกันด้านเทคนิค

(๑) จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบ (system security) ได้แก่ การรักษาความปลอดภัยทางเครือข่าย (network) และระบบสารสนเทศ (information technology systems) ซึ่งเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

(๒) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล (data security) ได้แก่ การตรวจสอบความปลอดภัยของข้อมูลที่เก็บไว้ในระบบ เพื่อให้แน่ใจว่ามีการควบคุมการเข้าถึงที่เหมาะสม และข้อมูลนั้นถูกเก็บไว้อย่างปลอดภัย

(๓) จัดให้มีการรักษาความมั่นคงปลอดภัยออนไลน์ (online security) ได้แก่ การรักษาความปลอดภัยทางเว็บไซต์ แอปพลิเคชัน หรือ บริการออนไลน์ต่างๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

(๔) จัดให้มีการรักษาความมั่นคงปลอดภัยของอุปกรณ์ (device security) ได้แก่ การรักษาความปลอดภัยของเครื่องมือหรืออุปกรณ์ที่เกี่ยวข้อง เช่น การควบคุมการใช้อุปกรณ์ภายนอกของบุคลากรหรือผู้ใช้บริการที่นำมาเชื่อมต่อกับอุปกรณ์ของมหาวิทยาลัย โดยการกำหนดนโยบายเกี่ยวกับการนำอุปกรณ์ของตนเองมาใช้ในการทำงาน หรือ Bring-your-own-Device (BYOD) เป็นต้น

(๕) กำหนดให้มีการตรวจสอบความถูกต้องของสิทธิ (authentication) สำหรับใช้ในการเข้าถึงระบบที่ใช้ประมวลผลข้อมูลส่วนบุคคล โดยปัจจัยที่ใช้ในการตรวจสอบความถูกต้องนั้นอาจอยู่ในรูปของ passwords, security tokens, หรือ biometrics เป็นต้น

(๖) ห้ามมิให้มีการติดตั้งซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย และห้ามมิให้ติดตั้งซอฟต์แวร์ผิดกฎหมายในระบบสารสนเทศของมหาวิทยาลัยโดยเด็ดขาด

(๗) การควบคุมและตรวจสอบการเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการขนส่งข้อมูล การถ่ายโอนข้อมูล การส่งผ่านข้อมูล หรือการจัดเก็บข้อมูลในอุปกรณ์จัดเก็บข้อมูล ทั้งทางวัสดุและทางอิเล็กทรอนิกส์ เช่น การกำหนดให้ข้อมูลที่สำคัญและละเอียดอ่อนทั้งหมดจะต้องถูกถ่ายโอนโดยใช้ช่องทางการสื่อสารที่มีการเข้ารหัสที่ปลอดภัย เช่น SSL Secured VPN, SFTP การเข้าถึงแอปพลิเคชันโดยใช้ https การแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัส (Encryption) เป็นต้น

ต่อหน้าที่ ๔ / (๘) การควบคุม...

(๘) การควบคุมความพร้อมใช้งานของข้อมูลส่วนบุคคล เพื่อให้ข้อมูลได้รับการคุ้มครองจากการถูกทำลายหรือสูญหายโดยมิได้เกิดจากความตั้งใจ เช่น การจัดให้มีซอฟแวร์ป้องกันไวรัสและความมั่นคงปลอดภัยจากส่วนกลาง กำหนดให้ข้อมูลที่สำคัญและละเอียดอ่อนซึ่งจัดเก็บไว้ในเซิร์ฟเวอร์นั้นต้องอยู่ในศูนย์ข้อมูลที่ปลอดภัยและได้รับการรับรอง กำหนดมาตรการเพื่อให้แน่ใจว่าข้อมูลพร้อมใช้งานอยู่ตลอดเวลา โดยเฉพาะด้านเครือข่าย (network) ที่สามารถรองรับการปฏิบัติงานในช่วงเวลาการทำงานสูงสุด และกำหนดให้มีการสำรองข้อมูลที่สำคัญทุกวัน เป็นต้น

๔.๑.๓ มาตรการป้องกันด้านกายภาพ

(๑) กำหนดให้มีการควบคุมการเข้าถึงอาคารสถานที่ หรืออุปกรณ์สำหรับจัดเก็บข้อมูลส่วนบุคคลและสถานที่ปฏิบัติงานของผู้ปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล เช่น การเข้า-ออกอาคารสถานที่โดยใช้กุญแจอิเล็กทรอนิกส์หรือคีย์การ์ดที่มอบให้เฉพาะบุคคล การกำหนดให้สถานที่สำคัญ เช่น ห้องเซิร์ฟเวอร์ ห้องจัดเก็บเอกสารข้อมูลส่วนบุคคล ต้องมีการล็อคประตูห้องเสมอและเข้าออกได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

(๒) กำหนดให้มีการระบุตัวตนของบุคคลที่ชัดเจนด้วยวิธีการที่เหมาะสม เช่น การแสดงบัตรประจำตัวของบุคลากรและบุคคลภายนอก การกำหนดอาณาบริเวณที่บุคลากรและบุคคลภายนอกสามารถเข้าถึงได้อย่างชัดเจน เป็นต้น

(๓) จัดให้มีการรักษาความปลอดภัยด้านอาคารสถานที่ อุปกรณ์สำหรับจัดเก็บข้อมูลส่วนบุคคล และสถานที่ปฏิบัติงานของผู้ปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล เช่น ตรวจตราคุณภาพของประตู หน้าต่าง กลอน ลูกบิดหรือแม่กุญแจให้อยู่ในสภาพดีเสมอ จัดให้มีเจ้าหน้าที่รักษาความปลอดภัย ไฟส่องสว่าง ระบบควบคุมอุณหภูมิและความชื้น ระบบสำรองไฟฟ้า ระบบและวัสดุอุปกรณ์ดับเพลิง ระบบป้องกันน้ำรั่วซึม ระบบยืนยันตัวบุคคลควบคุมการเข้าออก ระบบระฆังแจ้งเตือน (alarm) หรือ ระบบ CCTV เป็นต้น

(๔) จัดให้มีการตรวจสอบก่อนทิ้งหรือการจำหน่ายเอกสารหรืออุปกรณ์อิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้ว เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล

ข้อ ๕ ให้ผู้ควบคุมข้อมูลส่วนบุคคลรักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๗ สิงหาคม ๒๕๖๖

(ภราดาบัญชา แสงหิรัญ)
อธิการบดี

หมายเหตุ หากมีการตีความประกาศฉบับนี้ให้ถือฉบับภาษาไทยเป็นหลัก

สำนักงานบริหารทรัพยากรบุคคล