คำสั่งมหาวิทยาลัยอัสสัมชัญ

ที่ ๑๒๘/๒๕๖๖

เรื่อง แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล

ตามประกาศมหาวิทยาลัยอัสสัมชัญ ที่ ๑๒/๒๕๖๖ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖ ข้อ ๓ ได้มอบหมายให้ผู้ดำรงตำแหน่งรองอธิการบดี นายทะเบียน คณบดี ผู้อำนวยการ ทำหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคลมหาวิทยาลัยอัสสัมชัญ

เพื่อให้การดำเนินการของผู้ได้รับมอบหมายเป็นไปตามมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล อธิการบดีอาศัยอำนาจตามมาตรา ๔๓ แห่งพระราชบัญญัติสถาบันอุดมศึกษาเอกชน พ.ศ. ๒๕๔๖ แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๐ จึงกำหนดแนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับมอบหมาย ซึ่งต่อไปจะเรียกว่า “ท่าน” ไว้ดังนี้

ข้อ ๑ ตรวจสอบ พิจารณา การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของหน่วยงานที่ท่านรับผิดชอบ ให้เป็นไปตามวัตถุประสงค์ที่กำหนดในประกาศมหาวิทยาลัยอัสสัมชัญ ที่ ๑๒/๒๕๖๖

ข้อ ๒ กำกับดูแล/ควบคุม การรักษาความปลอดภัยของข้อมูลส่วนบุคคล ที่อยู่ในความรับผิดชอบของท่าน ให้เป็นไปตามประกาศมหาวิทยาลัยอัสสัมชัญ ที่ ๑๒/๒๕๖๖ โดย

๒.๑ **ด้านการบริหารจัดการ**

(๑) ให้กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลแก่บุคลากรในสังกัดของท่าน โดยกำหนดสิทธิการเข้าถึงข้อมูลแต่ละระดับตามหน้าที่ประมวลผลข้อมูล โดยกำหนดรหัส หรือมอบกุญแจตู้ ในกรณีข้อมูลถูกจัดเก็บในรูปแบบเอกสาร และจัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงเพื่อการประมวลผลข้อมูลในแต่ละระดับ ทบทวนสิทธิการเข้าถึงข้อมูลตลอดเวลาและปรับปรุงแก้ไขกรณีมีการเปลี่ยนแปลงสิทธิการเข้าถึงให้เป็นปัจจุบัน เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยตรวจสอบ

(๒) กำหนดเงื่อนไขการประมวลผลข้อมูลส่วนบุคคล เช่น จะเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลใดจะต้องขอความยินยอมจากเจ้าของข้อมูลอีกครั้ง เช่น การประมวลผลข้อมูลเพื่องานวิจัย หรือกำหนดให้การแก้ไข ย้าย หรือลบข้อมูลส่วนบุคคล ได้ต่อเมื่อได้รับอนุญาตจากท่านเป็นลายลักษณ์อักษร เป็นต้น

(๓) ควบคุม/ตรวจสอบการปฏิบัติตามเงื่อนไขที่กำหนด โดยจัดระบบที่สามารถรับรองได้ว่ามีการปฏิบัติตามเงื่อนไขทุกครั้ง เช่น ตรวจสอบข้อมูลย้อนกลับว่ามีข้อมูลส่วนบุคคลของบุคคลใดถูกเข้าถึง แก้ไข นำออกจากระบบ หรือถูกลบ

๒.๒ **มาตรการป้องกันด้านเทคนิค**

(๑) ประสานกับสำนักงานบริการเทคโนโลยีสารสนเทศ (ITS) เพื่อจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบ (system security) ความมั่นคงปลอดภัยของข้อมูล (data security) ความมั่นคงปลอดภัยออนไลน์ (online security) เช่น การจัดให้มีซอฟแวร์ป้องกันไวรัส หรือการแฮกข้อมูล เป็นต้น

(๒) ตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์ (device security) ที่ใช้ในหน่วยงานของท่าน เช่น การควบคุมการใช้อุปกรณ์ส่วนตัวของบุคลากร หรือผู้ใช้บริการ ที่นำมาเชื่อมต่อกับอุปกรณ์ โดยการกำหนดนโยบายเกี่ยวกับการนำอุปกรณ์ของตนเองมาใช้ในการทำงาน หรือ Bring-your-own-Device (BYOD) เป็นต้น

ต่อหน้าที่ ๒ / (๓) ตรวจสอบ...

(๓) ตรวจสอบความถูกต้องของสิทธิ (authentication) สำหรับใช้ในการเข้าถึงระบบที่ใช้ประมวลผลข้อมูลส่วนบุคคลในหน่วยงานของท่าน โดยปัจจัยที่ใช้ในการตรวจสอบความถูกต้องนั้นอาจอยู่ในรูปของ passwords, security tokens หรือ biometrics เป็นต้น

(๔) ตรวจสอบมิให้มีการติดตั้งซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงานท่าน รวมถึงมิให้ติดตั้งซอฟต์แวร์ผิดกฎหมายในระบบสารสนเทศของหน่วยงานท่านโดยเด็ดขาด

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

(๖) กำหนดมาตรการเพื่อให้แน่ใจว่าข้อมูลพร้อมจะใช้งานและสามารถตรวจสอบได้ตลอดเวลา เช่น เก็บข้อมูลส่วนบุคคลไว้ในเซิร์ฟเวอร์ที่ปลอดภัยและได้รับการรับรองว่าผู้ที่ท่านให้สิทธิเท่านั้นที่สามารถเข้าถึง กำหนดให้มีการสำรองข้อมูลที่สำคัญทุกวัน เป็นต้น

๒.๓ **มาตรการป้องกันด้านกายภาพ**

(๑) กำหนดให้มีการควบคุมการเข้าถึงห้องทำงานหรืออุปกรณ์สำหรับจัดเก็บข้อมูลส่วนบุคคล เช่น การเข้าออกห้องเซิร์ฟเวอร์ ห้องเก็บเอกสารโดยใช้กุญแจอิเล็กทรอนิกส์หรือคีย์การ์ดที่มอบให้เฉพาะบุคคล หรือต้องมีการล็อคประตูห้องเสมอและเข้าออกได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

(๒) จัดให้มีการรักษาความปลอดภัยห้องของผู้ปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล อุปกรณ์สำหรับจัดเก็บข้อมูลส่วนบุคคล เช่น ตรวจตราคุณภาพของประตู หน้าต่าง กลอน ลูกบิดหรือแม่กุญแจให้อยู่ในสภาพดีเสมอ ไฟส่องสว่าง ระบบควบคุมอุณหภูมิและความชื้น ระบบสำรองไฟฟ้า ระบบและวัสดุอุปกรณ์ดับเพลิง ระบบป้องกันน้ำรั่วซึม ระบบยืนยันตัวบุคคลควบคุมการเข้าออก ระบบระฆังแจ้งเตือน (alarm) หรือ ระบบ CCTV เป็นต้น

(๓) ตรวจสอบก่อนทิ้งหรือการจำหน่ายเอกสารหรืออุปกรณ์อิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้ว เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล

ข้อ ๓ ดำเนินงานในเรื่องอื่นๆ ดังนี้

๓.๑ แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลทันทีที่พบหรือได้รับรายงาน ต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลผ่านช่องทาง email: audpo@au.edu โดยใช้แบบฟอร์มตามเอกสารแนบท้ายคำสั่งนี้

๓.๒ จัดทำบันทึกรายงานการประมวลผลข้อมูลส่วนบุคคล (RoPA) เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตรวจสอบ

สั่ง ณ วันที่ ๗ สิงหาคม ๒๕๖๖

(ภราดาบัญชา แสงหิรัญ)
อธิการบดี

หมายเหตุ หากมีการตีความคำสั่งนี้ให้ถือฉบับภาษาไทยเป็นหลัก

สำนักงานบริหารทรัพยากรบุคคล