



ประกาศมหาวิทยาลัยสยาม  
เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล  
พ.ศ. ๒๕๖๙

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล มหาวิทยาลัยสยามในฐานะสถาบันอุดมศึกษาที่มีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบุคลากร นักศึกษา และบุคคลภายนอกเป็นจำนวนมาก ตระหนักถึงความสำคัญในการปฏิบัติตามกฎหมายดังกล่าว

อาศัยอำนาจตามความในมาตรา ๔๓ (๕) แห่งพระราชบัญญัติสถาบันอุดมศึกษาเอกชน พ.ศ. ๒๕๔๖ แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ มาตรา ๔๓ (๑) (๒) (๕) (๑๐) และ (๑๑) ประกอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จึงออกประกาศไว้ดังนี้

### หมวดที่ ๑ บททั่วไป

#### ข้อ ๑ นิยามศัพท์

ให้เป็นไปตามนิยามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยอนุโลม ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน เลขบัตรนักศึกษา ที่อยู่ หมายเลขโทรศัพท์ อีเมล ข้อมูลทางการศึกษา ข้อมูลทางการเงิน ภาพถ่ายและภาพเคลื่อนไหวจากกล้องโทรทัศน์วงจรปิด ลายเซ็นอิเล็กทรอนิกส์ และข้อมูลอื่นใดที่ทำให้สามารถระบุตัวบุคคลนั้นได้

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หมายความว่า ข้อมูลตามที่กฎหมายกำหนด เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน หรือข้อมูลพันธุกรรม

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า มหาวิทยาลัยสยาม ในฐานะผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล

“คณะกรรมการ” หมายความว่า คณะกรรมการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยสยาม

#### ข้อ ๒ ความมุ่งหมาย

ประกาศนี้มีวัตถุประสงค์เพื่อกำหนดกรอบแนวทางและหลักปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสยาม ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายที่เกี่ยวข้อง เพื่อสร้างความเชื่อมั่นแก่บุคลากร นักศึกษา ผู้ปกครอง และบุคคลภายนอก ว่ามหาวิทยาลัยให้ความสำคัญต่อสิทธิ ความเป็นส่วนตัวและความปลอดภัยของข้อมูลส่วนบุคคล

### ข้อ ๓ ขอบเขตการบังคับใช้

ประกาศนี้ใช้บังคับกับบุคลากรทุกประเภทของมหาวิทยาลัยสยาม รวมถึงคณาจารย์ พนักงาน มหาวิทยาลัย ข้าราชการ ลูกจ้าง นักศึกษา ผู้รับจ้าง ผู้ให้บริการ และคู่สัญญาทุกราย ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกิจการของมหาวิทยาลัย ไม่ว่าจะกระทำนั้นจะเกิดขึ้นภายในหรือภายนอกสถานที่ของมหาวิทยาลัย หรือในระบบสารสนเทศหรือนอกระบบสารสนเทศของมหาวิทยาลัยก็ตาม

### หมวดที่ ๒ หลักการพื้นฐาน

#### ข้อ ๔ หลักการคุ้มครองข้อมูลส่วนบุคคล

มหาวิทยาลัยมีนโยบายที่จะยึดมั่นในหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังต่อไปนี้

๑. หลักความถูกต้องชอบด้วยกฎหมาย โปร่งใส และเป็นธรรม (Lawfulness, Fairness and Transparency) — การเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้วยกฎหมาย มีความโปร่งใส และเป็นธรรม โดยต้องแจ้งวัตถุประสงค์และรายละเอียดที่เกี่ยวข้องให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวม

๒. หลักความจำกัดตามวัตถุประสงค์ (Purpose Limitation) — การเก็บรวบรวมข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์ที่ชัดเจน เฉพาะเจาะจง และชอบด้วยกฎหมาย โดยจะนำไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่แจ้งไว้ไม่ได้ เว้นแต่จะได้แจ้งให้เจ้าของข้อมูลทราบและได้รับความยินยอมหรือมีฐานทางกฎหมายอื่นรองรับ

๓. หลักความพอเพียงและไม่เกินความจำเป็น (Data Minimization) — การเก็บรวบรวมข้อมูลส่วนบุคคลต้องมีขอบเขตเท่าที่จำเป็นตามวัตถุประสงค์ ไม่เก็บรวบรวมไว้เกินความจำเป็น

๔. หลักความถูกต้องและเป็นปัจจุบัน (Accuracy) — มหาวิทยาลัยจะใช้ความพยายามอย่างสมเหตุสมผล เพื่อให้ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้มีความถูกต้อง เป็นปัจจุบัน และสมบูรณ์ โดยให้มีการตรวจสอบและปรับปรุงข้อมูลตามความเหมาะสม

๕. หลักการเก็บรักษาตามระยะเวลา (Storage Limitation) — ข้อมูลส่วนบุคคลจะถูกเก็บรักษาไว้ไม่เกินระยะเวลาที่จำเป็นตามวัตถุประสงค์แห่งการเก็บรวบรวม เมื่อพ้นกำหนดจะดำเนินการทำลายหรือลบข้อมูลให้หมดสิ้น

๖. หลักความมั่นคงปลอดภัย (Integrity and Confidentiality) — มหาวิทยาลัยจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลถูกเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยโดยมิชอบ

### หมวดที่ ๓ การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

#### ข้อ ๕ การเก็บรวบรวมและการขอความยินยอม

มหาวิทยาลัยมีนโยบายที่จะเก็บรวบรวมข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย โดยในกรณีที่ต้องขอความยินยอมจากเจ้าของข้อมูลเป็นฐานทางกฎหมาย มหาวิทยาลัยจะดำเนินการดังนี้

๑. จัดให้มีแบบขอความยินยอมเป็นลายลักษณ์อักษรหรือผ่านระบบอิเล็กทรอนิกส์ ที่แสดงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอย่างชัดเจน โดยไม่มีการหลอกลวงหรือบิดเบือนข้อเท็จจริง

๒. เปิดโอกาสให้เจ้าของข้อมูลสามารถให้หรือปฏิเสธความยินยอมได้โดยอิสระ โดยการปฏิเสธจะไม่ส่งผลกระทบต่อการใช้บริการขั้นพื้นฐานที่จำเป็นของมหาวิทยาลัย

๓. ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์หรือผู้ที่กฎหมายกำหนด ต้องได้รับความยินยอมจากผู้แทนโดยชอบธรรมตามกฎหมาย เว้นแต่กฎหมายจะอนุญาตให้ดำเนินการได้โดยไม่ต้องขอความยินยอม

๔. จัดให้มีช่องทางที่สะดวกให้เจ้าของข้อมูลสามารถถอนความยินยอมได้ตลอดเวลาที่ขอ โดยการถอนความยินยอมไม่ส่งผลกระทบต่อผลประโยชน์ที่ได้ดำเนินการไปแล้วก่อนการถอนความยินยอม

## **ข้อ ๖ การจัดทำทะเบียนข้อมูลส่วนบุคคลและบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)**

ให้เจ้าหน้าที่ผู้รับผิดชอบของแต่ละหน่วยงานดำเนินการจัดทำทะเบียนข้อมูลส่วนบุคคล (Data Inventory) และบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) ในส่วนงานที่ตนรับผิดชอบ เพื่อให้ทราบว่าหน่วยงานมีข้อมูลส่วนบุคคลอะไรบ้าง เก็บไว้ที่ใด นำไปใช้เพื่อวัตถุประสงค์ใด และมีการเปิดเผยแก่ใครบ้าง

ทั้งนี้ ให้ DPO เป็นผู้กำหนดแนวทาง รูปแบบ และแบบฟอร์มในการจัดทำดังกล่าว และให้หน่วยงานต่างๆ ส่งข้อมูลให้ DPO เพื่อรวบรวมเป็นทะเบียนข้อมูลส่วนบุคคลและบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในระดับมหาวิทยาลัย

## **ข้อ ๗ แหล่งที่มาและกิจกรรมการประมวลผล**

มหาวิทยาลัยอาจได้รับข้อมูลส่วนบุคคลจากแหล่งต่างๆ ดังนี้

๑. จากเจ้าของข้อมูลโดยตรง — ผ่านระบบต่างๆ ของมหาวิทยาลัย เช่น ระบบรับสมัครและคัดเลือก ระบบทะเบียนนักศึกษา ระบบบริหารทรัพยากรบุคคล ระบบเช็คเวลา ระบบลงทะเบียนเข้าร่วมกิจกรรม ระบบบริการสุขภาพและสวัสดิการ ตลอดจนระบบอื่นๆ ที่มหาวิทยาลัยจัดให้มีขึ้นตามความจำเป็นในการดำเนินการ

๒. จากบุคคลที่สาม — เช่น หน่วยงานภาครัฐ สถาบันการเงิน สถานศึกษาเดิม หรือหน่วยงานต้นสังกัดเดิม ตามความจำเป็นในการดำเนินการของมหาวิทยาลัย เช่น การตรวจสอบวุฒิการศึกษา การดำเนินการด้านเงินเดือนและสวัสดิการ หรือการประสานงานด้านสิทธิประโยชน์ต่างๆ

๓. จากระบบอัตโนมัติและระบบดิจิทัล — เช่น กล้องโทรทัศน์วงจรปิด (CCTV) ระบบบันทึกการใช้งานระบบสารสนเทศ (Log File) ระบบจดบันทึกการเข้า-ออกอาคาร หรือระบบอื่นๆ ที่มหาวิทยาลัยจัดให้มีขึ้นเพื่อความปลอดภัย การรักษาทรัพย์สิน และการบริหารจัดการพื้นที่ของมหาวิทยาลัย

ทั้งนี้ มหาวิทยาลัยมีนโยบายที่จะประมวลผลข้อมูลส่วนบุคคลเพื่อกิจกรรมหลักของมหาวิทยาลัย ดังนี้

(๑) การบริหารงานบุคคล — การรับสมัคร การคัดเลือก การบรรจุแต่งตั้ง การประเมินผล การพัฒนาบุคลากร การบริหารเงินเดือนและสวัสดิการ ตลอดจนการดำเนินการทางวินัยและการลาออก

(๒) การบริหารจัดการศึกษา — การรับสมัครนักศึกษา การขึ้นทะเบียนนักศึกษา การจัดการเรียนการสอน การวัดและประเมินผล การจัดกิจกรรมพัฒนานักศึกษา การให้บริการด้านสุขภาพและสวัสดิการ การจัดการทุนการศึกษา และการจัดทำเอกสารทางการศึกษา

(๓) การวิจัยและบริการวิชาการ — การดำเนินการวิจัย การเผยแพร่ผลงานวิชาการ การให้บริการวิชาการแก่สังคม และการสร้างนวัตกรรม

(๔) การบริหารจัดการทั่วไป — การบริหารงบประมาณ การพัสดุและทรัพย์สิน การบริหารอาคารสถานที่ การสื่อสารและประชาสัมพันธ์ของมหาวิทยาลัย และการพัฒนาระบบบริหารจัดการ

(๕) การดูแลรักษาทรัพย์สินในพื้นที่มหาวิทยาลัยและความปลอดภัยสาธารณะ — การควบคุมการเข้าออกพื้นที่ การเฝ้าระวังความปลอดภัยของทรัพย์สินและบุคคล การป้องกันและระงับเหตุอันตรายหรือเหตุฉุกเฉิน ตลอดจนการบริหารจัดการจราจรภายในมหาวิทยาลัย

ในการประมวลผลข้อมูลส่วนบุคคลเพื่อกิจกรรมต่างๆ ดังกล่าวข้างต้น มหาวิทยาลัยจะเลือกใช้ฐานทางกฎหมายที่เหมาะสมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้องกำหนด

#### ข้อ ๘ การเปิดเผยและการโอนข้อมูล

การเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม ไม่ว่าจะภายในหรือภายนอกมหาวิทยาลัย มหาวิทยาลัยจะกระทำเท่าที่จำเป็นตามวัตถุประสงค์และมีฐานทางกฎหมายรองรับ โดยจะแจ้งให้เจ้าของข้อมูลทราบถึงการเปิดเผยดังกล่าวตามความเหมาะสม

กรณีการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ มหาวิทยาลัยมีแนวทางที่จะดำเนินการให้เป็นไปตามที่กฎหมายกำหนด โดยจะตรวจสอบว่าประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอหรือไม่ และหากไม่มี มหาวิทยาลัยจะจัดให้มีมาตรการกำกับดูแลที่เหมาะสมเพื่อให้การคุ้มครองข้อมูลอยู่ในระดับที่เพียงพอ

#### ข้อ ๙ การจัดระดับข้อมูล

มหาวิทยาลัยมีนโยบายที่จะจัดระดับความลับของข้อมูลส่วนบุคคล เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับแต่ละระดับ ดังนี้

ระดับ	คำอธิบาย	ตัวอย่างข้อมูล
Public (สาธารณะ)	ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ โดยไม่ก่อให้เกิดความเสียหาย	ชื่อ-นามสกุล พร้อมตำแหน่งทางวิชาการ ข้อมูลการติดต่อในเว็บไซต์ทางการ
Internal (ภายใน)	ข้อมูลที่ใช้ภายในมหาวิทยาลัย เผยเฉพาะบุคลากรที่เกี่ยวข้อง	ตารางสอน รายชื่อบุคลากรภายใน ข้อมูลการประชุมภายใน
Confidential (ลับ)	ข้อมูลที่ต้องควบคุมการเข้าถึง เฉพาะผู้ที่มีอำนาจหน้าที่	ข้อมูลเงินเดือน ข้อมูลการประเมินผล ข้อมูลนักศึกษาส่วนบุคคล
Restricted (จำกัดสูงสุด)	ข้อมูลที่มีความอ่อนไหวสูง ต้องมีมาตรการรักษาความปลอดภัยเป็นพิเศษ	ข้อมูลสุขภาพ ข้อมูลประวัติอาชญากรรม ข้อมูลการสอบสวนทางวินัย

ทั้งนี้ มหาวิทยาลัยจะกำหนดให้หน่วยงานที่เกี่ยวข้องจัดทำแนวปฏิบัติในการจัดระดับข้อมูลและการเข้าถึงข้อมูลแต่ละระดับตามความเหมาะสม

## ข้อ ๑๐ ระยะเวลาเก็บรักษา

มหาวิทยาลัยมีนโยบายที่จะกำหนดระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลให้เหมาะสมกับแต่ละประเภทข้อมูล ตามที่กฎหมายกำหนดหรือตามหลักปฏิบัติที่ดี โดยมีระยะเวลาเก็บรักษาเบื้องต้น ดังนี้

ประเภทข้อมูล	ระยะเวลาเก็บรักษา	หมายเหตุ
ข้อมูลบุคลากร	ตลอดอายุการปฏิบัติงาน + ๑๐ ปี	ตามกฎหมายแรงงานและกฎหมายภาษีอากร
ข้อมูลนักศึกษา	ตลอดอายุการศึกษา + ๕ ปี	เพื่อประโยชน์ในการตรวจสอบและรับรองวุฒิ
ข้อมูลผู้สมัครงาน	๒ ปี	นับจากวันที่สมัคร
ภาพจากกล้องวงจรปิด (CCTV)	ไม่เกิน ๙๐ วัน	เว้นแต่มีเหตุจำเป็นตามกฎหมาย
ระบบบันทึกการใช้งาน (Log)	ไม่เกิน ๑๘๐ วัน	เว้นแต่มีเหตุจำเป็นตามกฎหมาย
ข้อมูลทางการเงิน	๑๐ ปี	ตามประมวลรัษฎากร
ผลการเรียนของนักศึกษา	ถาวร	เพื่อประโยชน์ในการตรวจสอบและรับรองวุฒิ
ข้อมูลอื่นๆ	ตามที่กฎหมายกำหนดหรือตามความจำเป็น	ตามวัตถุประสงค์แห่งการเก็บรวบรวม

เมื่อพ้นกำหนดระยะเวลาดังกล่าวข้างต้น มหาวิทยาลัยจะดำเนินการทำลายหรือลบข้อมูลส่วนบุคคลให้หมดสิ้น ด้วยวิธีการที่ไม่สามารถกู้คืนได้ เว้นแต่กฎหมายจะอนุญาตให้เก็บรักษาต่อไปได้

## หมวดที่ ๔ สิทธิของเจ้าของข้อมูล

### ข้อ ๑๑ สิทธิของเจ้าของข้อมูล

มหาวิทยาลัยมีนโยบายที่จะรับรองและอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิตามที่กฎหมายกำหนด ดังนี้

๑. สิทธิในการเข้าถึงและขอรับสำเนา — เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน เว้นแต่กรณีที่มีกฎหมายห้ามหรือมีเหตุอันควรปฏิเสธตามที่กฎหมายกำหนด ทั้งนี้ มหาวิทยาลัยจะแจ้งผลการพิจารณาให้เจ้าของข้อมูลทราบภายในระยะเวลาที่กฎหมายกำหนด

๒. สิทธิในการแก้ไขข้อมูลให้ถูกต้อง — เจ้าของข้อมูลมีสิทธิขอให้แก้ไขข้อมูลส่วนบุคคลที่ตนเห็นว่าไม่ถูกต้อง ไม่เป็นปัจจุบัน หรือไม่สมบูรณ์ โดยมหาวิทยาลัยจะดำเนินการแก้ไขหรือบันทึกคำคัดค้านไว้ให้แล้วเสร็จตามระยะเวลาที่กฎหมายกำหนด พร้อมแจ้งให้เจ้าของข้อมูลทราบผลการดำเนินการ

๓. สิทธิในการลบหรือทำลายข้อมูล — เจ้าของข้อมูลมีสิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของตนในกรณีที่ข้อมูลหมดความจำเป็นตามวัตถุประสงค์ เจ้าของข้อมูลถอนความยินยอม หรือในกรณีอื่นตามที่กฎหมายกำหนด เว้นแต่มหาวิทยาลัยจำเป็นต้องเก็บรักษาข้อมูลนั้นต่อไปตามกฎหมาย หรือเพื่อการก่อตั้งสิทธิเรียกร้องทางกฎหมาย หรือเพื่อเหตุอื่นตามที่กฎหมายอนุญาต

๔. สิทธิในการจำกัดการประมวลผล — เจ้าของข้อมูลมีสิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลของตนในกรณีที่อยู่ระหว่างการตรวจสอบความถูกต้องของข้อมูล ข้อมูลมีความจำเป็นเพียงเพื่อการก่อตั้งสิทธิเรียกร้องทางกฎหมาย หรือในกรณีอื่นตามที่กฎหมายกำหนด โดยมหาวิทยาลัยจะดำเนินการตามคำขอหรือแจ้งเหตุผลของการปฏิเสธให้เจ้าของข้อมูลทราบ

๕. สิทธิในการคัดค้านการประมวลผล — เจ้าของข้อมูลมีสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนในกรณีที่มหาวิทยาลัยประมวลผลโดยอาศัยฐานประโยชน์โดยชอบด้วยกฎหมาย หรือเพื่อวัตถุประสงค์ทางการตลาดโดยตรง เว้นแต่มหาวิทยาลัยจะมีเหตุอันชอบตามกฎหมายที่สำคัญกว่า หรือเพื่อการก่อตั้งสิทธิเรียกร้องทางกฎหมาย

๖. สิทธิในการขอให้โอนข้อมูล — เจ้าของข้อมูลมีสิทธิขอให้โอนข้อมูลส่วนบุคคลของตนที่มหาวิทยาลัยจัดทำไว้ในรูปแบบที่สามารถอ่านหรือใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ ไปยังผู้ควบคุมข้อมูลรายอื่นในกรณีที่กฎหมายกำหนด โดยมหาวิทยาลัยจะดำเนินการตามความเหมาะสมและขีดความสามารถที่มีอยู่

ทั้งนี้ การใช้สิทธิข้อ ๑-๖ ข้างต้น เจ้าของข้อมูลอาจยื่นคำขอได้ที่มหาวิทยาลัยสยาม โดยมหาวิทยาลัยจะดำเนินการตามคำขอภายในระยะเวลาที่กฎหมายกำหนด เว้นแต่มีเหตุอันควรปฏิเสธตามที่กฎหมายอนุญาต และจะแจ้งเหตุผลให้เจ้าของข้อมูลทราบ

## ข้อ ๑๒ ช่องทางการใช้สิทธิ

ให้เจ้าของข้อมูลส่วนบุคคลยื่นคำขอใช้สิทธิได้ที่มหาวิทยาลัยสยาม ตามช่องทางที่มหาวิทยาลัยประกาศกำหนด ซึ่งอาจรวมถึงการยื่นเป็นลายลักษณ์อักษร ณ สำนักงานที่เกี่ยวข้อง หรือการส่งคำขอผ่านระบบอิเล็กทรอนิกส์ตามที่มหาวิทยาลัยจัดให้มีขึ้น

ทั้งนี้ มหาวิทยาลัยจะดำเนินการตามคำขอโดยไม่ชักช้า และแล้วเสร็จภายในระยะเวลาที่กฎหมายกำหนด นับแต่วันที่ได้รับคำขอที่ถูกต้องครบถ้วน พร้อมแจ้งผลการดำเนินการให้เจ้าของข้อมูลทราบตามช่องทางที่แจ้งไว้

## หมวดที่ ๕ คณะกรรมการและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

### ข้อ ๑๓ การแต่งตั้ง

ให้อธิการบดีแต่งตั้งคณะกรรมการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลขึ้น โดยมีองค์ประกอบจากผู้ทรงคุณวุฒิหรือผู้มีความรู้ความเชี่ยวชาญในสาขาที่เกี่ยวข้อง และผู้บริหารหรือผู้แทนหน่วยงานที่เกี่ยวข้อง เพื่อทำหน้าที่กำกับดูแลและขับเคลื่อนนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย

ให้อธิการบดีแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) อย่างน้อย ๑ ท่าน ซึ่งมีความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายที่เกี่ยวข้อง เพื่อทำหน้าที่ให้คำแนะนำ ตรวจสอบ และประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

### ข้อ ๑๔ อำนาจหน้าที่

คณะกรรมการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจหน้าที่ดังต่อไปนี้

๑. กำหนดนโยบาย แนวปฏิบัติ มาตรการ และกลไกการตรวจสอบด้านการคุ้มครองข้อมูลส่วนบุคคล
๒. ติดตาม กำกับดูแล และประเมินผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลในมหาวิทยาลัย
๓. ทบทวนและปรับปรุงประกาศนี้ให้สอดคล้องกับกฎหมายและแนวปฏิบัติที่เปลี่ยนแปลงไป
๔. สนับสนุนและส่งเสริมการดำเนินงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ให้คำแนะนำ ตรวจสอบการดำเนินงานของมหาวิทยาลัยให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล จัดทำและปรับปรุงเอกสารที่เกี่ยวข้อง และประสานงานกับหน่วยงานกำกับดูแลตามที่กฎหมายกำหนด

## หมวดที่ ๖ มาตรการรักษาความมั่นคงปลอดภัย

### ข้อ ๑๕ มาตรการทั่วไป

มหาวิทยาลัยมีนโยบายที่จะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับระดับความเสี่ยงของข้อมูล โดยครอบคลุมมาตรการในสามระดับ ดังนี้

๑. มาตรการทางกายภาพ — เช่น การควบคุมการเข้าออกอาคารหรือพื้นที่จัดเก็บข้อมูล การใช้ระบบกล้องโทรทัศน์วงจรปิดในพื้นที่สำคัญ การรักษาความปลอดภัยของเอกสารและอุปกรณ์ที่จัดเก็บข้อมูล และการควบคุมการนำเข้าหรือนำออกอุปกรณ์ที่เกี่ยวข้อง

๒. มาตรการทางเทคนิค — เช่น การควบคุมการเข้าถึงระบบ (Access Control) การเข้ารหัสข้อมูล (Encryption) การตรวจสอบสิทธิ์การใช้งาน การบันทึกประวัติการเข้าถึงระบบ (Audit Log) และการป้องกันมัลแวร์และภัยคุกคามทางไซเบอร์ตามความเหมาะสม

๓. มาตรการทางบริหาร — เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบ (Need-to-Know Basis) การลงนามในสัญญาการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล การฝึกอบรมและสร้างความรู้ความเข้าใจแก่บุคลากร และการกำหนดบทลงโทษผู้ฝ่าฝืนตามข้อบังคับและระเบียบที่เกี่ยวข้อง

ทั้งนี้ การเลือกใช้มาตรการดังกล่าวให้เป็นไปตามความเหมาะสม ขนาด และทรัพยากรที่มีอยู่ของมหาวิทยาลัย

๓. บันทึกเหตุการณ์ — บันทึกเหตุละเมิดไว้เป็นหลักฐาน โดยระบุรายละเอียดของเหตุการณ์ วันเวลา ลักษณะการละเมิด ข้อมูลที่เกี่ยวข้อง การดำเนินการ และผลการประเมิน

๔. แจ้งหน่วยงานกำกับดูแล — ในกรณีที่การละเมิดก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล มหาวิทยาลัยจะแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้า แต่ไม่เกิน ๗๒ ชั่วโมง นับแต่ทราบเหตุ

๕. แจ้งเจ้าของข้อมูล — ในกรณีที่การละเมิดมีความเสี่ยงสูงต่อสิทธิและเสรีภาพ มหาวิทยาลัยจะแจ้งให้เจ้าของข้อมูลที่ได้รับผลกระทบทราบโดยไม่ชักช้า พร้อมทั้งแจ้งแนวทางแก้ไขและเยียวยาที่เหมาะสม

#### หมวดที่ ๗ บทเฉพาะกาล

##### ข้อ ๑๘ การทบทวนนโยบาย

มหาวิทยาลัยมีนโยบายที่จะทบทวนประกาศนี้อย่างน้อยทุกๆสามปี เว้นแต่จะมีเหตุจำเป็นหรือมีการเปลี่ยนแปลงของกฎหมายหรือแนวปฏิบัติที่สำคัญ ซึ่งคณะกรรมการอาจพิจารณาทบทวนก่อนกำหนดก็ได้ โดยให้คณะกรรมการเป็นผู้พิจารณาความเหมาะสมและรับฟังความคิดเห็นจากผู้มีส่วนเกี่ยวข้องเพื่อนำมาประกอบการปรับปรุง

##### ข้อ ๑๙ การบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๕ มกราคม พ.ศ. ๒๕๖๔



(ดร.พรชัย มงคลวนิช)

อธิการบดี