



ประกาศสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
(KMITL Privacy Policy)

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (“สถาบัน”) ให้ความสำคัญกับความเป็นส่วนตัวของนักศึกษา บุคลากรและบุคคลอื่นที่เกี่ยวข้องกับสถาบัน เพื่อให้เกิดความมั่นใจว่าบุคคลดังกล่าวจะได้รับความคุ้มครองสิทธิอย่างครบถ้วนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พระราชบัญญัติ”) นโยบายฉบับนี้จะอธิบายเกี่ยวกับการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่สถาบันประมวลผล การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การกำกับมาตรการการคุ้มครองข้อมูลส่วนบุคคล บทบาท หน้าที่และความรับผิดชอบของสถาบัน และบทลงโทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน จึงประกาศออกมาเพื่อให้สถาบันมีหลักเกณฑ์ กลไก มาตรการกำกับดูแล และการบริหารจัดการข้อมูลส่วนบุคคลอย่างชัดเจนและเหมาะสม

อาศัยอำนาจตามความในข้อ 4 วรรคสอง ของข้อบังคับสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ประกอบกับมติที่ประชุมคณะกรรมการเพื่อเตรียมความพร้อมในการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการประชุมครั้งที่ 6/2565 เมื่อวันที่ 19 พฤษภาคม พ.ศ. 2565 จึงให้ประกาศดังนี้

ข้อ 1 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 2 ขอบเขตการบังคับใช้

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ ใช้กับบุคลากรของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และบุคคลอื่นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสถาบัน

ข้อ 3 คำนิยาม

3.1 การประมวลผล (Processing) หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น การเก็บรวบรวม บันทึก จัดระบบ ทำโครงสร้าง เก็บรักษา ปรับปรุง เปลี่ยนแปลง คุ้มครอง ใช้ เผยแพร่ ส่งต่อ เผยแพร่ โอน ผสมเข้าด้วยกัน ลบ ทำลาย

3.2 ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวตนของบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ IP Address รูปภาพ เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง ข้อมูลทางพันธุกรรม ข้อมูลทางชีวภาพ (Biometric data)

3.3 เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลธรรมดาที่ข้อมูลส่วนบุคคลสามารถระบุตัวตนของบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

3.4 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลธรรมดาหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

3.5 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลธรรมดาหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อ 4 นโยบายการคุ้มครองข้อมูลส่วนบุคคล : ด้านการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Governance)

4.1 สถาบันจะจัดให้มีโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล เพื่อกำหนดวิธีการและมาตรการที่เหมาะสมในการปฏิบัติตามพระราชบัญญัติ ดังนี้

(1) กำหนดให้มีโครงสร้างองค์กร (Organizational Structure) หรือกระบวนการงาน (Work Process) รวมทั้งกำหนดบทบาท ภารกิจและความรับผิดชอบของหน่วยงานและผู้ปฏิบัติงานที่เกี่ยวข้องให้ชัดเจน เพื่อสร้างกลไกการกำกับดูแล การควบคุม ความรับผิดชอบ การปฏิบัติงาน การบังคับใช้ และการติดตาม มาตรการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

(2) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสถาบัน (KMITL Data Protection Officer: KMITL DPO) โดยมีบทบาทและหน้าที่ตามที่กำหนดในข้อบังคับสถาบันว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

4.2 สถาบันจะจัดทำนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล และข้อบังคับสถาบันว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

4.3 สถาบันจะจัดให้มีกระบวนการบริหารการปฏิบัติตามนโยบาย (Policy Management Process) เพื่อควบคุมดูแลให้มีการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบันอย่างต่อเนื่อง

4.4 สถาบันจะดำเนินการฝึกอบรมบุคลากรของสถาบัน เพื่อให้บุคลากรของสถาบันตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และทำให้มั่นใจได้ว่าพนักงานของสถาบันที่เกี่ยวข้องทุกคนผ่านการอบรม และมีความรู้ความเข้าใจในการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

ข้อ 5 นโยบายการคุ้มครองข้อมูลส่วนบุคคล : ด้านการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing)

5.1 สถาบันจะประมวลผลข้อมูลส่วนบุคคล ทั้งในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและหรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยคำนึงถึงความถูกต้องของข้อมูลส่วนบุคคล ทั้งนี้ การกำหนดขอบเขตวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลและระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล ให้ทำได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายและแนวทางการดำเนินงานของสถาบัน อีกทั้งสถาบันจะดำเนินการรักษาความลับ ความถูกต้องสมบูรณ์ และความปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอ

5.2 สถาบันจะดำเนินการและรักษาบันทึกการประมวลผลข้อมูลส่วนบุคคล (Records of Processing: RoP) สำหรับบันทึกรายการและกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมทั้งจะปรับปรุงบันทึกการประมวลผลข้อมูลส่วนบุคคล เมื่อมีการเปลี่ยนแปลงรายการหรือกิจกรรมที่เกี่ยวข้อง

5.3 สถาบันจะจัดให้มีกลไกการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล รวมทั้งจัดให้มีกลไกการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

5.4 ในกรณีที่สถาบันส่ง โอน หรือให้บุคคลอื่นใช้ข้อมูลส่วนบุคคล สถาบันจะจัดทำข้อตกลงกับผู้รับหรือใช้ข้อมูลส่วนบุคคลนั้นเพื่อกำหนดสิทธิและหน้าที่ให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

5.5 สถาบันจะลบ หรือทำให้ข้อมูลไม่สามารถระบุไปยังเจ้าของข้อมูลส่วนบุคคลได้ เมื่อครบกำหนดระยะเวลา โดยปฏิบัติให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและแนวทางการดำเนินงานของสถาบัน

5.6 สถาบันจะประเมินความเสี่ยงและจัดทำมาตรการเพื่อบรรเทาความเสี่ยงและลดผลกระทบที่จะเกิดขึ้นกับการประมวลผลข้อมูลส่วนบุคคล

ข้อ 6 นโยบายการคุ้มครองข้อมูลส่วนบุคคล : ด้านการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

สถาบันจะจัดให้มีช่องทางและวิธีการเพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนได้ตามที่กฎหมายกำหนด รวมทั้งจะดำเนินการบันทึกและประเมินผลการตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ข้อ 7 นโยบายการคุ้มครองข้อมูลส่วนบุคคล : ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Personal Data Security)

7.1 สถาบันจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอ รวมทั้งดำเนินการป้องกันไม่ให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลและการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต

7.2 สถาบันจะจัดให้มีนโยบายการบริหารจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Privacy Incident Management Policy) และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Program) เพื่อให้สามารถระบุและจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างทันที่

ข้อ 8 นโยบายการคุ้มครองข้อมูลส่วนบุคคล : ด้านการกำกับให้เกิดการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Compliance)

สถาบันจะจัดให้มีการทบทวนและปรับปรุงนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำ เพื่อให้ทันสมัยสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและสถานการณ์ในแต่ละช่วงเวลา

ข้อ 9 บทบาท หน้าที่และความรับผิดชอบของบุคลากรของสถาบัน

9.1 หน่วยงานภายในสถาบัน มีบทบาท หน้าที่และความรับผิดชอบดังต่อไปนี้

(1) ดำเนินการให้มีโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล เพื่อให้เกิดการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

(2) กำกับดูแลและสนับสนุนให้สถาบันดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพและสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

9.2 ผู้บริหาร มีบทบาท หน้าที่ และความรับผิดชอบในการติดตามควบคุมให้หน่วยงานที่ดูแลปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน และส่งเสริมการสร้างวัฒนธรรมที่รู้ทันกับพนักงานของสถาบัน

9.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสถาบัน (KMITL DPO) มีบทบาท หน้าที่และความรับผิดชอบตามที่กฎหมายกำหนด ซึ่งรวมถึงหน้าที่ดังต่อไปนี้

(1) รายงานสถานการณ์คุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสถาบันทราบอย่างสม่ำเสมอ และจัดทำข้อเสนอแนะเพื่อปรับปรุงการคุ้มครองข้อมูลส่วนบุคคลของสถาบันให้ทันสมัยและสอดคล้องกับกฎหมายอยู่เสมอ

(2) ให้คำแนะนำบุคลากรของสถาบันเกี่ยวกับกรปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

(3) ตรวจสอบการดำเนินงานของหน่วยงานในสถาบัน ให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

9.4 บุคลากรของสถาบันมีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

(1) ปฏิบัติให้สอดคล้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(2) รายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน ให้ผู้บังคับบัญชาทราบ

ข้อ 10 โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน

สถาบันกำหนดให้หน่วยงานหรือบุคลากรของสถาบันที่เกี่ยวข้องกับข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างเคร่งครัด หากไม่ปฏิบัติหรือฝ่าฝืนตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสถาบัน อาจมีความผิดและถูกลงโทษทางวินัยตามข้อบังคับของสถาบัน และอาจต้องรับโทษตามที่กฎหมายกำหนด

ประกาศ ณ วันที่ ๒๕๖๕ พฤษภาคม พ.ศ. ๒๕๖๕



(รองศาสตราจารย์อโนวัฒน์ จางวนิชเลิศ)
รักษาการแทนอธิการบดี