คู่มือการปฏิบัติตามนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคล
เพื่อใช้อบรมสร้างความตระหนักและให้ความรู้เป็นการภายใน สจล. ประจำปี 2569

สารบัญ

1. บทนำ

คู่มือนี้จัดทำขึ้นเพื่อใช้อบรมสร้างความตระหนักและให้ความรู้เป็นการภายใน สำหรับผู้ปฏิบัติงานในสถาบัน และผู้ที่เกี่ยวข้องของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เพื่อให้การจัดการข้อมูลส่วนบุคคลเป็นไปตามหลักกฎหมาย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และปฏิบัติได้จริง เน้นในงานด้านบริหารทรัพยากรบุคคล (HR) และในงานด้านทะเบียนนักศึกษา (KRESO) โดยเนื้อหาครอบคลุมแนวทางปฏิบัติ แบบฟอร์มที่พร้อมใช้ ตารางระยะเวลาเก็บรักษา และแบบบันทึกการดำเนินการ (RoPA)

2. วัตถุประสงค์ ขอบเขต และอธิบายศัพท์สำคัญ

2.1 วัตถุประสงค์

2.1.1 เสริมสร้างความรู้ ความเข้าใจเชิงปฏิบัติแก่ผู้ปฏิบัติงานในสถาบัน และผู้ที่เกี่ยวข้องของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) รวมถึงแนวทางและมาตรการปฏิบัติของสถาบันอย่างถูกต้องและเหมาะสม

2.1.2 จัดทำและเตรียมแบบฟอร์มมาตรฐานสำหรับบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) รวมถึงตารางกำหนดระยะเวลาการเก็บรักษาข้อมูล (Retention Schedule) ในรูปแบบตัวอย่าง สำหรับสำนักงานบริหารทรัพยากรบุคคล และสำนักทะเบียนและบริการการศึกษา

2.1.3 ลดความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล และเตรียมความพร้อมในการดำเนินการตอบสนองต่อคำร้องหรือเหตุการณ์ที่เกี่ยวข้องอย่างเป็นระบบและมีประสิทธิภาพ

2.2 ขอบเขต

2.2.1 ครอบคลุมการดำเนินการประมวลผลข้อมูลส่วนบุคคลของกลุ่มบุคคลที่เกี่ยวข้องกับการดำเนินงานของสถาบัน ได้แก่ บุคลากร ผู้สมัครงาน นักศึกษา ผู้ปกครอง ผู้ให้บริการภายนอก ตลอดจนผู้ติดต่อและผู้มีส่วนเกี่ยวข้องอื่น ๆ ที่เกี่ยวข้องกับภารกิจของสถาบัน

2.3 อธิบายศัพท์สำคัญ

2.3.1 **ข้อมูลส่วนบุคคล** คือ ข้อมูลที่สามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

2.3.2 **ข้อมูลอ่อนไหว** คือ ข้อมูลเกี่ยวกับเชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง สุขภาพ/พันธุกรรม ฯลฯ

2.3.3 **ผู้ควบคุมข้อมูล** คือ หน่วยงาน/บุคคลที่กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูล

2.3.4 **ผู้ประมวลผลข้อมูล** คือ หน่วยงาน/บุคคลที่ประมวลผลข้อมูลในนามของผู้ควบคุมข้อมูล

2.3.5 **ความยินยอม** คือ การกระทำหรือคำแสดงเจตนาชัดแจ้งจากเจ้าของข้อมูลที่ยินยอมให้มีการประมวลผล

3. หลักการและข้อกำหนดแนวทางปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

3.1 หลักการสำคัญ

ทุกครั้งก่อนเปิดโครงการ/บริการใหม่ ในกรณีที่ต้องมีการประมวลผลข้อมูลส่วนบุคคลในปริมาณมาก หรือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว หรือมีการโอนข้อมูลส่วนบุคคลออกนอกประเทศ หน่วยงานควรดำเนินการประเมินความจำเป็นและจัดทำกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อวิเคราะห์และประเมินความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) พร้อมกำหนดมาตรการในการป้องกันและลดความเสี่ยงอย่างเหมาะสมก่อนเริ่มดำเนินการ

3.2 แนวทางปฏิบัติทั่วไป

3.2.1 **ปฏิบัติถูกต้องตามกฎหมาย:** ก่อนเริ่มเก็บรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคล ควรกำหนดฐานทางกฎหมายให้ชัดเจน เช่น การปฏิบัติตามสัญญา การปฏิบัติหน้าที่ตามกฎหมาย ประโยชน์โดยชอบด้วยกฎหมายของสถาบัน หรือความยินยอมของเจ้าของข้อมูลส่วนบุคคล เป็นต้น พร้อมทั้งจัดทำบันทึกและระบุรายละเอียดดังกล่าวไว้ในแบบฟอร์มโครงการหรือเอกสารประกอบกิจกรรม

3.2.2 **โปร่งใส** แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล วิธีการหรือช่องทางการใช้ข้อมูล รวมถึงระยะเวลาในการเก็บรักษาข้อมูล ผ่านประกาศความเป็นส่วนตัว (Privacy Notice) ที่มีความชัดเจนเหมาะสม และสอดคล้องกับบริบทของการติดต่อกับเจ้าของข้อมูลส่วนบุคคลแต่ละกลุ่ม อาทิ นักศึกษา บุคลากร ผู้ปกครอง และบุคคลภายนอกสถาบัน

3.2.3 **จำกัดวัตถุประสงค์และความจำเป็นให้น้อยสุด** เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นต่อการดำเนินงานตามวัตถุประสงค์ที่ได้กำหนดไว้เท่านั้น และห้ามนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่แจ้งไว้ โดยไม่มีฐานทางกฎหมายรองรับหรือมีการแจ้งให้ทราบก่อนล่วงหน้า

3.2.4 **ความถูกต้องของข้อมูล** กำหนดกระบวนการและแนวปฏิบัติสำหรับการอัปเดตข้อมูลส่วนบุคคล รวมถึงการดำเนินการตอบสนองต่อคำขอแก้ไขข้อมูลจากเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสมและสอดคล้องกับข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

3.2.5 **จำกัดการเก็บรักษา** กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลไว้ในนโยบาย/ตารางเก็บรักษา และดำเนินการทำลาย หรืออำพรางข้อมูลเมื่อครบกำหนดระยะเวลาตามเงื่อนไขที่กำหนดไว้

3.2.6 **ความมั่นคงปลอดภัย** ให้มีการกำหนดและดำเนินมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งในด้านการบริหารจัดการ ด้านเทคนิค และด้านกายภาพ เช่น การควบคุมสิทธิ์การเข้าถึงข้อมูล การเข้ารหัสและถอดรหัสลับ การสำรองข้อมูล ตลอดจนมาตรการอื่นที่จำเป็น เพื่อป้องกันการเข้าถึง ใช้ เปิดเผย แก้ไข หรือทำลายข้อมูลโดยมิชอบหรือโดยไม่ได้รับอนุญาต

3.2.7 **ความรับผิดชอบและการบันทึก** ให้มีการจัดทำและบันทึกรายละเอียดกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ใน บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) อย่างครบถ้วน พร้อมกำหนดและมอบหมายผู้รับผิดชอบในการดูแลข้อมูลส่วนบุคคลในแต่ละชุดอย่างชัดเจน

3.3 ตัวอย่างการใช้ฐานกฎหมาย

3.3.1 **ฐานภารกิจของรัฐ (Public Task)**

ใช้เมื่อ ประมวลผลข้อมูลนักศึกษาและการเรียนการสอน

วิธีปฏิบัติ เก็บหลักฐานการอ้างอิงข้อกฎหมายและผู้ที่อนุมัติการให้ข้อมูลส่วนบุคคล

3.3.2 **ฐานหน้าที่ตามกฎหมาย (Legal Obligation)**

ใช้เมื่อ การส่งรายงานภาครัฐ การปฏิบัติตามกฎข้อบังคับของกระทรวงฯ

วิธีปฏิบัติ เก็บหลักฐานการอ้างอิงข้อกฎหมายและผู้ที่อนุมัติการให้ข้อมูลส่วนบุคคล

3.3.3 **ฐานผลประโยชน์ชอบด้วยเหตุผลของสถาบัน (Legitimate Interest)**

ใช้เมื่อ สถิติการบริหาร งานเฝ้าระวังความปลอดภัยภายในตัวอาคาร

วิธีปฏิบัติ ดำเนินการให้สมดุล และบันทึกเหตุผลประกอบการตัดสินใจ

3.3.4 **ฐานสัญญา (Contractual Necessity)**

ใช้เมื่อ การรับเข้าทำงาน การลงทะเบียนวิชา การออกใบรับรอง

วิธีปฏิบัติ ระบุในสัญญาหรือข้อผูกพันว่าเก็บและใช้ข้อมูลส่วนบุคคลใดเพื่อการปฏิบัติหน้าที่

3.3.5 **ฐานจดหมายเหตุ/วิจัย/สถิติ (Historical/Research/Statistic Base)**

ใช้เมื่อ ประมวลผลข้อมูลส่วนบุคคลแบบนิรนามหรือเฉลี่ยกลุ่ม เพื่อลดการขอความยินยอม

วิธีปฏิบัติ ดำเนินการให้สมดุล และบันทึกเหตุผลประกอบการตัดสินใจ

3.3.6 **ฐานความยินยอม (Consent)**

ใช้เมื่อ แบบฟอร์มสมัคร อีเมลส่งข่าวส่งเสริมกิจกรรมเลือกเข้าร่วม บริการเสริมที่ไม่จำเป็นต่อสัญญาหรือหน้าที่

วิธีปฏิบัติ

1. ใช้ข้อความขอความยินยอมชัดเจน แจกแจงประเภทข้อมูล/วัตถุประสงค์ และบันทึกวันที่เวลา แหล่งที่มา พร้อมทั้งเปิดโอกาสให้เพิกถอนโดยสะดวก
2. กรณีเจ้าของข้อมูลส่วนบุคคลอายุไม่เกิน 10 ปี ต้องได้รับความยินยอมจากผู้แทนโดยชอบธรรม
3. กรณีเจ้าของข้อมูลส่วนบุคคลอายุเกินกว่า 10 ปี ให้ขอความยินยอมจากผู้แทนโดยชอบธรรม ให้เหมาะสมกับลักษณะและวัตถุประสงค์ของกิจกรรมนั้น

3.4 แบบฟอร์มและเอกสารแม่แบบที่เกี่ยวข้อง

3.4.1 เอกสารแม่แบบ Privacy Notice

3.4.2 แบบฟอร์มขอความยินยอม (Consent Form)

3.4.3 แบบคำร้องขอใช้สิทธิ์เจ้าของข้อมูล (DSR Form)

3.4.4 เอกสารแม่แบบ RoPA

3.4.5 ตารางแม่แบบ Retention Schedule

4. ขั้นตอนปฏิบัติเมื่อจะเริ่มโครงการ/บริการใหม่ (DPIA Workflow)

กระบวนการดังกล่าวได้รับการออกแบบเพื่อสนับสนุนให้ผู้ปฏิบัติงานในสถาบัน และผู้ที่เกี่ยวข้องของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง สามารถดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเป็นระบบ ตั้งแต่ขั้นตอนการริเริ่มแนวคิดโครงการ ตลอดจนการติดตามและประเมินผลภายหลังการใช้งาน เพื่อให้การดำเนินงานเป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และสอดคล้องกับหลักความรับผิดชอบในการกำกับดูแลข้อมูลส่วนบุคคลของหน่วยงาน

4.1 ตรวจประเมินเบื้องต้น (DPIA Pre-Screening)

ผู้รับผิดชอบโครงการ (Project Owner) ต้องกรอกแบบฟอร์มประเมินเบื้องต้น ก่อนเริ่มออกแบบหรือจัดทำระบบ โดยแบบฟอร์มต้องรวบรวมข้อมูลขั้นต่ำดังนี้

4.1.1 ชื่อโครงการ/บริการ หน่วยงานเจ้าของ ผู้จัดการโครงการ และผู้ติดต่อประสานงาน

4.1.2 วัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล

4.1.3 ประเภทข้อมูลส่วนบุคคลที่คาดว่าจะเก็บ/ใช้ ทั้งระดับปกติและระดับอ่อนไหว

4.1.4 กลุ่มเจ้าของข้อมูล เช่น นักศึกษา บุคลากร ภายนอก

4.1.5 ช่องทางและวิธีการเก็บข้อมูล เช่น ออนไลน์ แอปพลิเคชัน ฟอร์มกระดาษ

4.1.6 ขนาดและช่วงเวลาเก็บข้อมูล คือ ปริมาณโดยประมาณ และเป็นการเก็บถาวรหรือเพียงชั่วคราว

4.1.7 มีการใช้ผู้ประมวลผลภายนอกหรือไม่ (Vendor/Cloud)

4.1.8 คาดว่าอาจมีความเสี่ยงสูงต่อสิทธิพื้นฐานหรือไม่ หลังจากนั้นตอบคำถามสั้น ๆ สำหรับ Pre-Screening (ใช่/ไม่/ไม่แน่ใจ)

4.1.9 รวบรวมข้อมูลเชิงอัตลักษณ์เฉพาะบุคคล (เช่น บัตรประชาชน) หรือข้อมูลสุขภาพหรือไม่?

4.1.10 ใช้การติดตามเชิงพิกัด พฤติกรรม หรือการตัดสินใจโดยอัตโนมัติหรือไม่?

4.1.11 ข้อมูลแบ่งปันกับหน่วยงานภายนอกหรือข้ามประเทศหรือไม่?

4.1.12 มีการเก็บข้อมูลจำนวนมาก (เช่น มากกว่า 1,000 คน) หรือไม่? แล้วพิจารณาแปรผลการ Pre-Screening

4.1.13 หากทุกข้อเป็น “ไม่” และไม่มีลักษณะการประมวลผลเชิงเสี่ยง ให้บันทึกผลในระบบภายในและสามารถดำเนินโครงการต่อได้โดยไม่ต้องทำ DPIA ฉบับเต็ม

4.1.14 หากมีข้อใดข้อหนึ่งเป็น “ใช่” หรือ “ไม่แน่ใจ” ให้ดำเนินการทำ DPIA ฉบับเต็ม

4.2 ประเมินความเสี่ยง (DPIA)

4.2.1 โครงสร้างเนื้อหา DPIA ฉบับเต็ม ควรมีหัวข้ออย่างน้อย ดังนี้

4.2.1.1 บทนำและขอบเขตโครงการ

4.2.1.2 คำอธิบายการประมวลผล คือ ข้อมูลที่เก็บ วิธีการ ประเภทการประมวลผล

4.2.1.3 วัตถุประสงค์ทางกฎหมายของการประมวลผล (ฐานทางกฎหมาย ความยินยอม, สัญญา, หน้าที่ตามกฎหมาย, ผลประโยชน์ชอบด้วยกฎหมาย ฯลฯ)

4.2.1.4 การระบุและวิเคราะห์ความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล สำหรับแต่ละความเสี่ยงให้ระบุ

1. ความเป็นไปได้ (Low/Medium/High)

2. ผลกระทบ (Minor/Moderate/Severe)

3. บทสรุปเหตุการณ์ที่อาจเกิดขึ้น

4.2.1.5 มาตรการลดความเสี่ยงที่เสนอ (Technical & Organizational Controls)

4.2.1.6. การประเมินความเหลืออยู่ของความเสี่ยง (Residual Risk) หลังมาตรการ

4.2.1.7 แผนการตรวจสอบและการทบทวน (KPIs, ระยะเวลา)

4.2.1.8 การมีส่วนร่วมของผู้เกี่ยวข้องและการให้ข้อมูลแก่เจ้าของข้อมูล (Data Subject Rights)

4.2.1.9 บันทึกการตัดสินใจและลายเซ็นผู้อนุมัติ

4.2.2 วิธีการวิเคราะห์ความเสี่ยง

4.2.2.1 ระบุเหตุการณ์ไม่พึงประสงค์ ไม่ว่าจะเป็นการรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต หรือการใช้ข้อมูลในทางที่ผิด

4.2.2.2 ประเมินระดับความร้ายแรงของผลกระทบ เช่น ผลต่อชื่อเสียง ความเป็นส่วนตัว การเงิน ความปลอดภัยทางร่างกาย เป็นต้น

4.2.2.3 ให้คะแนนความเป็นไปได้และผลกระทบ แล้วคำนวณระดับความเสี่ยง ตัวอย่างตารางคะแนน 3x3 หรือ 5x5 เพื่อให้ชัดเจน

4.3 กำหนดมาตรการลดเสี่ยง (Technical & Organizational Controls)

4.3.1 แนวทางมาตรการควรจัดเป็นหมวดหมู่ชัดเจน

4.3.1.1 การควบคุมเชิงเทคนิค

1. การเข้ารหัสลับข้อมูลขณะส่งและจัดเก็บ อาทิ TLS, AES-256
2. การจัดการสิทธิ์แบบ Least Privilege และ Role-based Access Control
3. การยืนยันตัวตนแบบหลายปัจจัยสำหรับผู้ดูแลระบบ (MFA for Admin)
4. การบันทึกและตรวจสอบการเข้าถึง (Audit Logging) พร้อมการเก็บล็อกอย่างปลอดภัย
5. การแยกข้อมูลทดสอบกับข้อมูลจริง
6. การสำรองข้อมูลและแผนกู้คืน (Backup & DRP)

4.3.1.2 การควบคุมเชิงบริหาร

1. นโยบายการเข้าถึงและการใช้ข้อมูล และข้อตกลงการรักษาความลับ (NDA) สำหรับผู้ที่เกี่ยวข้อง
2. กระบวนการจัดการคำร้องขอสิทธิของเจ้าของข้อมูล คือกิจกรรมเข้าถึง แก้ไข และลบข้อมูล
3. การอบรมผู้ใช้งานเฉพาะที่เกี่ยวข้องกับระบบ
4. การตรวจสอบผู้ให้บริการภายนอก (Vendor assessment & Data Processing Agreement)
5. กำหนดผู้รับผิดชอบชัดเจนสำหรับการตรวจสอบและรายงานเหตุการณ์

4.3.2 ตัวอย่างกรณีมาตรการเฉพาะกิจ

4.3.2.1 หากระบบมีการประมวลผลข้อมูลสุขภาพ ต้องจำกัดสิทธิ์เฉพาะบุคลากรที่จำเป็น เข้ารหัสลับทั้งช่องทางและฐานข้อมูล และเก็บล็อกแบบละเอียด

4.3.2.2 หากแชร์ข้อมูลข้ามประเทศ ต้องตรวจสอบกฎหมายประเทศที่รับข้อมูลและใส่ข้อกำหนดการคุ้มครองในสัญญา

4.4 ตรวจสอบและประเมิน

4.4.1 ขั้นตอนการส่ง

4.4.1.1 Project Owner ส่ง DPIA ฉบับเต็มพร้อมแบบฟอร์มสรุปความเสี่ยง (Executive Summary) ให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือคณะทำงานที่เกี่ยวข้อง

4.4.1.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตรวจสอบความครบถ้วนของเอกสารและประเมินว่ามาตรการเพียงพอหรือไม่

4.4.1.3 หากจำเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะขอข้อมูลหรือให้คำแนะนำเพิ่มเติม

4.4.1.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทำหน้าที่รวบรวมและจัดทำรายงานสรุปเพื่อนำเสนอต่อสภาสถาบันหรือหน่วยงานตรวจสอบที่เกี่ยวข้อง

4.4.2 เกณฑ์การประเมิน ตัวอย่าง

4.4.2.1 ความเสี่ยง residual ต้องอยู่ในระดับที่ยอมรับได้ตามนโยบายสถาบัน

4.4.2.2 มีมาตรการทางเทคนิคและบริหารรองรับอย่างน้อยสำหรับความเสี่ยงระดับสูงที่ถูกระบุ

4.4.2.3 ผู้ให้บริการภายนอกมี DPA และผ่านการประเมินความปลอดภัยเบื้องต้น

4.4.3 การยกระดับกรณีความเสี่ยงสูง

4.4.3.1 หาก residual risk ยังคงสูงถึงระดับที่ไม่ยอมรับได้ ต้องส่งเรื่องให้คณะผู้บริหารระดับสูง เพื่อพิจารณาตัดสินใจเชิงนโยบาย

4.5 บันทึกและติดตามผล

4.5.1 บันทึกผลใน RoPA (Record of Processing Activities):

4.5.1.1 ข้อมูลที่ต้องบันทึกจาก DPIA อาทิ ชื่อโครงการ วัตถุประสงค์ ประเภทข้อมูล ผู้รับผิดชอบ ขอบเขตการเข้าถึง มาตรการที่นำมาใช้ ผลการประเมินความเสี่ยง วันที่อนุมัติ

4.5.1.2 RoPA ต้องสามารถค้นหาและส่งออกเพื่อการตรวจสอบภายในและการตรวจสอบภายนอกได้ง่าย

4.5.2 การติดตามและทบทวนมาตรการ

4.5.2.1 กำหนดรอบการทบทวนมาตรการหลังเปิดใช้งานอย่างน้อยทุก 6 เดือนสำหรับโครงการที่มีความเสี่ยงสูง และสำหรับความเสี่ยงต่ำทุก 12 เดือน

4.5.2.2 ทบทวนเมื่อมีการเปลี่ยนแปลงสำคัญ เช่น ขยายขอบเขตการประมวลผล เปลี่ยนผู้ให้บริการภายนอก หรือพบเหตุการณ์ละเมิดข้อมูล

4.5.2.3 จัดทำรายงานสรุปผลการติดตาม (Monitoring Report) และอัพเดต DPIA หากมีการเปลี่ยนแปลงหรือหาก residual risk เพิ่มขึ้น

4.5.3 การเก็บรักษาเอกสาร

4.5.3.1 ต้องเก็บ DPIA และเอกสารที่เกี่ยวข้องไว้ไม่น้อยกว่าเวลาที่กฎหมายกำหนด

4.6 แนวทางปฏิบัติที่เป็นประโยชน์และตัวอย่างแบบฟอร์ม/เช็คลิสต์

4.6.1 เช็คลิสต์ย่อสำหรับผู้กรอก pre-screening จำนวนหนึ่งหน้า มีรายละเอียดดังต่อไปนี้

4.6.1.1 ข้อมูลที่รวบรวมเป็นข้อมูลส่วนบุคคลอ่อนไหวหรือไม่

4.6.1.2 มีการประมวลข้อมูลส่วนบุคคลอัตโนมัติที่ส่งผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลหรือไม่

4.6.1.3 ข้อมูลจะถูกเปิดเผยนอกสถาบันหรือไม่

4.6.1.4 จำเป็นต้องเก็บข้อมูลนานกว่า 5 ปีหรือไม่

4.6.1.5 มีการฝากข้อมูลไว้ที่ Vendor/Cloud หรือไม่

4.6.2 แบบฟอร์มสรุปมาตรการ (สำหรับแนบ DPIA)

4.6.2.1 ระบุมาตรการแต่ละข้อ, ประเภท (เทคนิค/บริหาร), ผู้รับผิดชอบ, กำหนดเวลาในการนำไปปฏิบัติ, สถานะ (Planned/In progress/Implemented)

4.6.3 ตัวอย่าง KPI สำหรับการติดตาม

4.6.3.1 จำนวนเหตุการณ์ละเมิดข้อมูลต่อปีและสาเหตุ

4.6.3.2 เวลาตอบสนองต่อคำร้องสิทธิเจ้าของข้อมูล (เฉลี่ยวัน)

4.6.3.3 จำนวนการทบทวนและการอัปเดต DPIA ตามกำหนด

4.6.4 การอบรมและการสื่อสาร

4.6.4.1จัดอบรมเชิงปฏิบัติการให้ Project Owner และทีมพัฒนาเกี่ยวกับการกรอก pre-screeningการอ่าน DPIA และการจัดการคำร้องสิทธิ

4.6.4.2 จัดคู่มือสั้น (1-2 หน้า) สำหรับหัวข้อที่พบบ่อย เช่น การทำ DPA กับ Vendor, การเข้ารหัสลับข้อมูล, การตั้งสิทธิ์ผู้ใช้

หัวข้อสรุปการยกระดับความรับผิดชอบ

1. Project Owner ต้องรับผิดชอบการกรอกแบบฟอร์ม Pre-Screening ส่ง DPIA และติดตามการนำมาตรการไปปฏิบัติ
2. IT/ผู้ดูแลระบบ (KDMC) ต้องออกแบบและนำมาตรการทางเทคนิคไปใช้ และให้ข้อมูลทางเทคนิคแก่ DPO
3. DPO/คณะทำงาน พิจารณา DPIA และให้คำแนะนำหรือยกระดับกรณีความเสี่ยงสูง
4. รองอธิการบดี/คณบดี พิจารณาแนวทางการดำเนินงานในกรณีที่ยังมีความเสี่ยงคงเหลือภายหลังการดำเนินการจัดทำ DPIA

5. ตัวอย่างการจัดชั้นข้อมูลและระยะเวลาเก็บรักษาเชิงปฏิบัติ

ตัวอย่างการจัดชั้นข้อมูลและระยะเวลาเก็บรักษาเชิงปฏิบัติสำหรับสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ตารางแนวปฏิบัติการจัดชั้นข้อมูลและระยะเวลาเก็บรักษา

6. มาตรการความมั่นคงปลอดภัยเชิงปฏิบัติ

สถาบันในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่กำหนดมาตรการองค์กร (Organizational Controls) ขั้นต่ำ เพื่อใช้เป็นแนวทางในการบริหารจัดการและคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. กำหนดนโยบายการเข้าถึงข้อมูลและการกำหนดสิทธิการใช้งาน (Access Control Policy)

2. กำหนดหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (Separation of Duties) อย่างเหมาะสม เพื่อป้องกันและลดความเสี่ยงจากการใช้อำนาจหรือการปฏิบัติหน้าที่เกินขอบเขตที่ได้รับมอบหมาย

3. จัดให้มีกระบวนการบริหารจัดการด้านการจ้างงาน และการสิ้นสุดการปฏิบัติงานอย่างเหมาะสม เพื่อให้มีการทบทวนสิทธิการเข้าถึงข้อมูลส่วนบุคคล เมื่อมีการเปลี่ยนตำแหน่ง หรือพ้นสภาพการปฏิบัติงาน

4. จัดทำข้อตกลงหรือสัญญากับพันธมิตร ผู้ให้บริการ หรือผู้ประมวลผลข้อมูลส่วนบุคคลภายนอก รวมถึงข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้ชัดเจนและเหมาะสม

นอกจากนี้ สถาบันมีความจำเป็นต้องกำหนดแนวปฏิบัติที่ชัดเจน เป็นมาตรฐานเดียวกัน และสามารถนำไปใช้ปฏิบัติได้จริงสำหรับผู้ปฏิบัติงานในสถาบัน และผู้ที่เกี่ยวข้องของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เพื่อให้การจัดเก็บ การใช้ และการเปิดเผยข้อมูลส่วนบุคคลของผู้เกี่ยวข้องเป็นไปโดยชอบด้วยกฎหมาย โดยแนวปฏิบัติดังกล่าวครอบคลุมในด้านนโยบาย ขั้นตอนการปฏิบัติงาน บทบาทและหน้าที่ความรับผิดชอบ ตลอดจนตัวชี้วัดและแนวทางการตรวจสอบ ซึ่งสามารถสรุปได้ดังนี้

1. การควบคุมการเข้าถึง กำหนดให้มีการทบทวนสิทธิการเข้าถึงข้อมูลและระบบตามบทบาทหน้าที่ (Role-based Access Control) อย่างสม่ำเสอม โดยต้องดำเนินการทบทวนสิทธิทุก 6-12 เดือน

2. การพิสูจน์ตัวตน กำหนดให้มีการใช้รหัสผ่านที่มีความมั่นคงปลอดภัยในระดับสูง และใช้การยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) สำหรับระบบที่ใช้เข้าถึงข้อมูลส่วนบุคคลอย่างละเอียด เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3. การเข้ารหัสลับ กำหนดให้มีการเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลสำคัญหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว ทั้งในระหว่างการรับส่งข้อมูล และในระหว่างการจัดเก็บข้อมูล เพื่อป้องกันการเข้าถึง การเปิดเผย หรือการใช้งานข้อมูลโดยไม่ได้รับอนุญาต

4. การสำรองข้อมูลและการกู้คืน กำหนดให้มีนโยบายและกระบวนการสำรองข้อมูล พร้อมดำเนินการทดสอบการกู้คืนข้อมูล อย่างน้อยปีละ 1 ครั้ง

5. การล็อกและบันทึกเหตุการณ์ กำหนดให้มีการจัดเก็บบันทึกการเข้าถึงข้อมูล สำหรับกิจกรรมที่สำคัญอย่างน้อย 1 ปี พร้อมกำหนดกระบวนการตรวจสอบติดตาม เพื่อรองรับการตรวจสอบย้อนหลังและการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างเหมาะสม

6. การลบ/ทำลายข้อมูล: กำหนดแนวทางและวิธีการทำลายข้อมูลทั้งในรูปแบบกายภาพและดิจิทัล เหมาะสม และสามารถตรวจสอบได้ โดยต้องมีการบันทึกหลักฐานการดำเนินการทำลายข้อมูล เช่น การลบข้อมูลแบบถาวรด้วยวิธีเขียนทับข้อมูล (wipe/overwrite) หรือการทำลายสื่อบันทึกข้อมูลทางกายภาพ (Physical Shredding) เพื่อป้องกันการกู้คืนหรือการนำข้อมูลกลับมาใช้งานโดยไม่ได้รับอนุญาต

6.1 การควบคุมการเข้าถึง

6.1.1 **หลักการ** กำหนดสิทธิการเข้าถึงข้อมูลตามหลักการ "เท่าที่จำเป็นต่อการปฏิบัติงาน" และ "สิทธิการเข้าถึงตามบทบาทหน้าที่" เพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่มีหน้าที่และความจำเป็นในการใช้งานข้อมูลตามภารกิจที่ได้รับมอบหมายเท่านั้น

6.1.2 **บทบาทและความรับผิดชอบ**

6.1.2.1 **เจ้าของข้อมูล (Data Owners)** อาทิ หัวหน้างานฝ่ายทะเบียน หัวหน้าฝ่ายบุคคล หรือผู้แทนหน่วยงาน มีหน้าที่กำหนดประเภทของข้อมูล ระดับชั้นข้อมูล และสิทธิการเข้าถึงข้อมูลสำหรับชุดข้อมูลที่อยู่ภายใต้ความรับผิดชอบ

6.1.2.2 **ผู้ดูแลข้อมูล (Data Stewards)** มีหน้าที่จัดทำและปรับปรุงรายการข้อมูล กำหนดตารางสิทธิการเข้าถึงข้อมูล (Access Matrix) รวมถึงประสานงาน และดำเนินการทบทวนสิทธิการเข้าถึงข้อมูลให้เป็นไปตามนโยบายและบทบาทหน้าที่ที่กำหนดไว้

6.1.2.3 **ผู้ดูแลระบบเทคโนโลยีสารสนเทศ (IT Administrators)** มีหน้าที่บริหารจัดการและกำหนดค่าการควบคุมสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ เช่น Access Control List (ACL) และ Role-Based Access Control (RBAC) รวมถึงติดตั้ง ดูแลรักษา และตรวจสอบมาตรการควบคุมด้านเทคนิค (Technical Controls)

6.1.3 **กระบวนการปฏิบัติ**

6.1.3.1 จัดทำตารางกำหนดสิทธิการเข้าถึงข้อมูล (Access Matrix) แยกตามระบบสารสนเทศและชุดข้อมูล เช่น ข้อมูลนักศึกษา ข้อมูลบุคลากร ข้อมูลวิจัย

6.1.3.2 กำหนดให้การอนุมัติสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศต้องได้รับการพิจารณาและอนุมัติโดยหัวหน้าหน่วยงาน พร้อมจัดเก็บหลักฐานและบันทึกข้อมูลผ่านระบบบริหารจัดการคำขอสิทธิการใช้งาน (Access Request/Ticketing System) อย่างเหมาะสม

6.1.3.3 ดำเนินการตรวจสอบและทบทวนรายการผู้มีสิทธิใช้งานระบบอย่างสม่ำเสมอ อย่างน้อย 6-12 เดือน โดยผู้ดูแลข้อมูล (Data Stewards) และจัดทำรายงานผลการทบทวนเสนอต่อผู้บริหารระดับสูง

6.1.3.4 กำหนดกระบวนการเพิกถอน ระงับ หรือปรับเปลี่ยนสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศโดยทันที เมื่อบุคลากรมีการย้ายหน่วยงาน ลาออก พ้นสภาพการปฏิบัติงาน หรือมีการเปลี่ยนแปลงบทบาทหน้าที่

6.2 การพิสูจน์ตัวตน

6.2.1 **กำหนดนโยบายรหัสผ่าน (Password Policy)** ให้ผู้ใช้งานกำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า 12 ตัวอักษร และมีความซับซ้อนเพียงพอเพื่อป้องกันการคาดเดาหรือการโจมตีทางไซเบอร์ รวมถึงห้ามใช้รหัสผ่านใหม่ซ้ำกับรหัสผ่านที่เคยใช้งานก่อนหน้า

6.2.2 **กำหนดให้มีการใช้การยืนยันตัวตนแบบ Multi-Factor Authentication (MFA)** สำหรับระบบสารสนเทศที่ใช้จัดเก็บ ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความสำคัญ มีรายละเอียด หรือปริมาณมาก เช่น ระบบทะเบียน ระบบเงินเดือน และระบบสารสนเทศด้านบุคลากร

6.2.3 **การบริหารจัดการบัญชีพิเศษ** บัญชีผู้ดูแลและบัญชีผู้บริการอื่นๆ ต้องกำหนดอายุการใช้งานของรหัสผ่าน บันทึกเหตุผลในการใช้งาน รวมถึงมีการตรวจสอบและทบทวนบันทึกการใช้งานย้อนหลังอย่างสม่ำเสมอ

6.2.4 **กิจกรรมเพิ่มเติม**

6.2.4.1 กำหนดให้ผู้ใช้งานใหม่ต้องดำเนินการลงทะเบียนการยืนยันตัวตนแบบหลายปัจจัย (Muli-Factor Authentication: MFA) ภายในระยะเวลาไม่เกิน 15 วัน นับจากวันที่ได้รับสิทธิการเข้าใช้งาน

6.2.4.2 จัดให้มีกระบวนการรีเซ็ตรหัสผ่านที่มีความมั่นคงปลอดภัย อาทิ การดำเนินการผ่าน Helpdesk พร้อมการยืนยันตัวตนแบบหลายปัจจัย

6.2.4.3 จัดให้มีการอบรมและสร้างความตระหนักแก่ผู้ใช้งานทั่วไปเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยเฉพาะการโจมตีในรูปแบบฟิชชิง (Phishing) รวมถึงขั้นตอนการแจ้งรายงานเหตุการณ์หรือความผิดปกติด้านความมั่นคงปลอดภัยต่อหน่วยงานที่เกี่ยวข้อง

6.3 การเข้ารหัสลับ

6.3.1 **นโยบายการเข้ารหัสลับ**

6.3.1.1 ข้อมูลสำคัญและข้อมูลอ่อนไหวต้องได้รับการเข้ารหัสลับทั้งในขณะจัดเก็บข้อมูล (Data at Rest) และในขณะรับส่งข้อมูล (Data in Transit)

6.3.1.2 ใช้มาตรฐานการเข้ารหัสที่เป็นที่ยอมรับในระดับสากล เช่น TLS เวอร์ชัน 1.2 ขึ้นไป สำหรับการสื่อสารข้อมูล และ AES-256 สำหรับการเข้ารหัสลับข้อมูลที่จัดเก็บอยู่ในระบบ

6.3.2 **การบริหารจัดการกุญแจเข้ารหัส (Key Management System: KMS)**

6.3.2.1 ต้องมีระบบบริหารจัดการกุญแจเข้ารหัส (Key Management System: KMS) แยกออกจากระบบจัดเก็บข้อมูล พร้อมกำหนดนโยบายการหมุนเวียนกุญแจเข้ารหัส (Key Rotation) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดเหตุการณ์ที่มีความเสี่ยงสูงด้านความมั่นคงปลอดภัยสารสนเทศ

6.3.2.2 ต้องมีการจัดเก็บบันทึกการเข้าถึงและการใช้งานกุญแจเข้ารหัส เพื่อรองรับการตรวจสอบและติดตามย้อนหลังได้

6.3.3 **กิจกรรมเพิ่มเติม**

6.3.3.1 ต้องมีการตรวจสอบความถูกต้องและความมั่นคงปลอดภัยของการเชื่อมต่อผ่าน TLS/SSL อย่างสม่ำเสมอ และควรใช้ใบรับรองที่ถูกต้องและเชื่อถือได้สำหรับบริการที่เปิดให้ใช้งานสาธารณะ

6.3.3.2 ต้องกำหนดรายการไฟล์หรือฐานข้อมูลที่จำเป็นต้องเข้ารหัสลับ รวมถึงบันทึกมาตรฐานการเข้ารหัสที่ใช้ไว้ในทะเบียนข้อมูลหรือเอกสารที่เกี่ยวข้องอย่างชัดเจน

6.4 การสำรองข้อมูลและการกู้คืน

6.4.1 **นโยบายสำรองข้อมูล**

6.4.1.1 ต้องกำหนดความถี่ในการสำรองข้อมูลตามความสำคัญของข้อมูล เช่น สำรองข้อมูลรายสัปดาห์สำหรับข้อมูลทะเบียนและข้อมูลเงินเดือน และสำรองข้อมูลรายเดือนสำหรับข้อมูลทั่วไป

6.4.1.2 ต้องจัดเก็บสำเนาข้อมูลสำรองอย่างน้อย 3 ชุด บนสื่อจัดเก็บข้อมูลหรือสถานที่ที่แตกต่างกัน ตามหลักการ 3-2-1 (3 Copies / 2 Media Types / 1 Offsite) ได้แก่ การมีข้อมูลสำรอง 3 ชุด ใช้สื่อจัดเก็บอย่างน้อย 2 ประเภท และจัดเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

6.4.2 **การทดสอบกู้คืน**

6.4.2.1 ต้องดำเนินการทดสอบการกู้คืนข้อมูลและระบบอย่างน้อยปีละ 1 ครั้ง พร้อมจัดทำบันทึกผลการทดสอบ โดยครอบคลุมระยะเวลาในการกู้คืนสภาพ และปัญหาที่พบ

6.4.2.2 ต้องจัดทำคู่มือหรือแนวปฏิบัติการกู้คืนระบบ (Runbook) สำหรับระบบสารสนเทศที่สำคัญ ประกอบด้วยขั้นตอนการดำเนินงานโดยสรุป ผู้รับผิดชอบในแต่ละส่วนงาน และคำสั่งหรือวิธีการที่เกี่ยวข้องกับการกู้คืนระบบอย่างชัดเจน

6.4.3 **การจัดเก็บสำรอง**

6.4.3.1 ต้องดำเนินการสำรองข้อมูลในรูปแบบที่มีการเข้ารหัสลับ และกำหนดข้อมูลกำกับ (Metadata) อย่างน้อย ได้แก่ วันที่ดำเนินการ ผู้รับผิดชอบดำเนินการ และค่า Checksum เพื่อใช้ในการตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง

6.4.4 **ตัวชี้วัด**

6.4.4.1 ต้องกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ (Recover Time Objective: RTO) และระดับข้อมูลสูญหายที่ยอมรับได้ (Recovery Point Objective: RPO) สำหรับแต่ละระบบหรือบริการอย่างชัดเจน

6.5 การล็อกและบันทึกเหตุการณ์

6.5.1 **ขอบเขตการล็อก**

6.5.1.1 ต้องจัดทำบันทึกเหตุการณ์ (Log) อย่างน้อยครอบคลุมการเข้าสู่ระบบ การเข้าถึงฐานข้อมูล การเปลี่ยนแปลงสิทธิผู้ใช้งาน การดาวน์โหลดหรือส่งออกข้อมูล ตลอดจนกิจกรรมที่ดำเนินการโดยผู้ดูแลระบบ

6.5.2 **ระยะเวลาการเก็บ**

6.5.2.1 จัดเก็บบันทึกเหตุการณ์ (Log) สำหรับเหตุการณ์สำคัญไว้เป็นระยะเวลาไม่น้อยกว่า 1 ปี และกำหนดนโยบายการเก็บรักษาข้อมูล (Retention Policy) อย่างชัดเจน เพื่อให้สอดคล้องกับระดับความเสี่ยง และข้อกำหนดทางกฎหมาย

6.5.3 **กระบวนการตรวจสอบ**

6.5.3.1 กำหนดการแจ้งเตือน (Alert) สำหรับเหตุการณ์หรือกิจกรรมที่ผิดปกติ เช่น การพยายามเข้าสู่ระบบหลายครั้งติดต่อกัน ความพยายามเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการส่งออกข้อมูลในปริมาณมากผิดปกติ

6.5.3.2 กำหนดให้มีการทบทวนและตรวจสอบบันทึกเหตุการณ์ (Log) โดยหน่วยงานหรือทีมงานด้านความมั่นคงปลอดภัยอย่างน้อยทุก 6 เดือน พร้อมจัดทำรายงานสรุปผลการตรวจสอบเสนอต่อผู้บริหารอย่างน้อยปีละ 1 ครั้ง

6.5.4 **การเก็บรักษาและการปกป้อง**

6.5.4.1 จัดเก็บบันทึกเหตุการณ์ (Log) ไว้ในระบบที่แยกออกจากระบบต้นทาง และมีมาตรการป้องกันการแก้ไข โดยใช้เทคโนโลยีประเภท Immutability หรือ WORM (Write Once Read Many) Storage ตามความเหมาะสม

6.5.5 **ขั้นตอนเมื่อพบเหตุผิดปกติ**

6.5.5.1 กำหนดให้มีการระบุ คัดแยก และประเมินระดับความรุนแรงของเหตุการณ์ (Triage)

6.5.5.2 กำหนดให้มีการแจ้งเหตุไปยังทีมตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response Team) ภายในระยะเวลาที่กำหนด

6.5.5.3 กำหนดให้มีการเก็บรักษาบันทึกเหตุการณ์และหลักฐาน เพื่อรองรับการสืบสวน การตรวจสอบย้อนหลัง และการรายงานตามข้อกำหนดของกฎหมาย

6.6 การลบและทำลายข้อมูล

6.6.1 **นโยบายการเก็บรักษา**

6.6.1.1 กำหนดระยะเวลาในการจัดเก็บข้อมูลให้ชัดเจนตามประเภทของข้อมูล โดยให้สอดคล้องกับข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ และนโยบายของสถาบัน

6.6.2 **วิธีการทำลายข้อมูลดิจิทัล**

6.6.2.1 กำหนดให้ใช้วิธีการลบหรือทำลายข้อมูลอย่างปลอดภัยตามมาตรฐานที่ยอมรับได้ เช่น การเขียนทับข้อมูลซ้ำ (Overwrite) หรือการทำลายข้อมูลด้วยวิธี Cryptographic Erase ในกรณีที่มีการใช้การเข้ารหัสด้วยกุญแจเข้ารหัสที่สามารถหมุนเวียนได้

6.6.2.2 กำหนดให้จัดเก็บบันทึกการทำลายข้อมูล โดยอย่างน้อยต้องระบุวันที่ดำเนินการ ผู้รับผิดชอบดำเนินการ และวิธีการที่ใช้ในการทำลายข้อมูล

6.6.3 **วิธีการทำลายข้อมูลทางกายภาพ**

6.6.3.1 ดำเนินการทำลายเอกสารด้วยเครื่องตัดย่อยเอกสารในระดับความปลอดภัยที่เหมาะสม และจัดเก็บบันทึกการทำลายเอกสาร โดยอย่างน้อยต้องระบุวันที่ดำเนินการ ปริมาณและประเภทของเอกสาร รวมถึงผู้อนุมัติการทำลาย

6.6.4 **ขั้นตอนการอนุมัติการทำลาย**:

6.6.4.1 เจ้าของข้อมูลที่รับผิดชอบจัดทำคำขออนุมัติการทำลายข้อมูล พร้อมระบุเหตุผลและหลักฐานประกอบว่าได้ครบระยะเวลาที่กำหนดแล้ว

6.6.4.2 ผู้มีอำนาจอนุมัติ เช่น หัวหน้าแผนกหรือเจ้าหน้าที่ด้านความปลอดภัย ตรวจสอบความถูกต้องและพิจารณาอนุมัติการทำลายข้อมูล

6.6.4.3 ดำเนินการทำลายข้อมูลตามวิธีการที่กำหนด พร้อมจัดเก็บบันทึกผลการดำเนินการไว้เป็นหลักฐาน

6.7 กิจกรรมเพิ่มเติม

6.7.1 **การตรวจสอบภายใน**

6.7.1.1 ดำเนินการตรวจสอบการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Adherence) อย่างน้อยปีละ 1 ครั้ง โดยหน่วยงานตรวจสอบภายในหรือหน่วยงานที่ได้รับมอบหมาย

6.7.1.2 จัดทำบันทึกผลการตรวจสอบ ช่องว่างหรือข้อบกพร่องที่พบ รวมถึงแผนการปรับปรุงแก้ไข และติดตามผลการดำเนินงานจนกว่าจะสามารถปิดประเด็นข้อบกพร่องได้ครบถ้วน

6.7.2 **การทดสอบความปลอดภัยเชิงรุก**

6.7.2.1 ดำเนินการทดสอบเจาะระบบ (Penetration Test) และประเมินช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (Vulnerability Assessment) สำหรับระบบสารสนเทศที่มีความสำคัญตามระดับความเสี่ยงและงบประมาณ อย่างน้อยปีละ 1 ครั้ง

6.7.3 **การฝึกอบรมบุคลากร**

6.7.3.1 จัดให้มีการอบรมเพื่อสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ สำหรับผู้ปฏิบัติงานในสถาบันและผู้ที่เกี่ยวข้องของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นประจำทุกปี พร้อมจัดให้มีแบบทดสอบเพื่อประเมินความเข้าใจภายหลังการอบรม

6.7.3.2 จัดให้มีการอบรมเชิงปฏิบัติการสำหรับผู้ดูแลข้อมูล (Data Stewards) และผู้ดูแลระบบ (IT Administrator) เป็นประจำทุกปี

6.7.4 **ตัวชี้วัดการปฏิบัติงาน**

6.7.4.1 อัตราการทบทวนสิทธิ์การเข้าถึงที่แล้วเสร็จภายในระยะเวลาที่กำหนด จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบและได้รับการแก้ไข ระยะเวลาเฉลี่ยในการตอบสนองต่อเหตุการณ์ และผลการทดสอบการกู้คืนข้อมูล

7. กระบวนการตอบสนองต่อคำขอของเจ้าของข้อมูล

7.1 รับคำขอ ระบุช่องทางรับคำขอ เช่น E-mail แบบฟอร์มออนไลน์ หรือจุดให้บริการ พร้อมบันทึกวันที่และรายละเอียดการรับคำขอไว้เป็นหลักฐาน

7.2 ระบุตัวบุคคล ดำเนินการตรวจสอบและยืนยันตัวตนของผู้ยื่นคำขอด้วยวิธีการที่เหมาะสม เช่น การตรวจสอบเอกสารประจำตัว หรือระบบยืนยันตัวตน

7.3 ประเมินคำขอ ประเมินและพิจารณาประเภทของคำขอ เช่น การขอเข้าถึงข้อมูล การขอแก้ไขข้อมูล การขอลบข้อมูล เป็นต้น รวมถึงตรวจสอบฐานกฎหมายที่เกี่ยวข้อง

7.4 ดำเนินการภายในกำหนดเวลา ดำเนินการตามคำขอภายในระยะเวลาที่กฎหมายกำหนด

7.5 บันทึกและสื่อสารผล แจ้งผลการดำเนินการแก่ผู้ยื่นคำขอเป็นลายลักษณ์อักษร พร้อมจัดเก็บบันทึกการดำเนินงานการพิจารณา และเหตุผลประกอบกรณีมีการปฏิเสธคำขอ

8. การจัดการเหตุการณ์ละเมิดข้อมูล

8.1 ทีมตอบสนอง กำหนดทีมตอบสนองต่อเหตุการณ์ข้อมูลรั่วไหลหรือเหตุละเมิดข้อมูลส่วนบุคคล เช่น ฝ่ายเทคโนโลยีสารสนเทศ (IT) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ฝ่ายกฎหมาย และฝ่ายสื่อสารองค์กร พร้อมกำหนดลำดับและช่องทางการติดต่อในกรณีฉุกเฉิน

8.2 ขั้นตอนเบื้องต้น ดำเนินการตอบสนองเบื้องต้นโดยแยกระบบที่ได้รับผลกระทบ ยับยั้งหรือควบคุมการรั่วไหลของข้อมูล และจัดเก็บบันทึกเหตุการณ์หรือหลักฐานที่เกี่ยวข้อง

8.3 ประเมินผลกระทบ โดยวิเคราะห์ระดับความรุนแรง ขอบเขตของผลกระทบ และจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ

8.4 แจ้งหน่วยงานและเจ้าของข้อมูล ดำเนินการแจ้งหน่วยงานกำกับดูแลและเจ้าของข้อมูลส่วนบุคคลตามกระบวนการและระยะเวลาที่กำหนดไว้ รวมถึงแจ้งเจ้าของข้อมูลเมื่อมีความจำเป็น

8.5 ถอดบทเรียนและแก้ไข จัดทำรายงานสรุปสาเหตุการณ์ วิเคราะห์สาเหตุของปัญหา พร้อมปรับปรุงมาตรการควบคุมและทบทวนกระบวนการป้องกัน

9. บทบาทความรับผิดชอบ

9.1 ผู้ปฏิบัติงานในสถาบัน และผู้ที่เกี่ยวข้องของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (Data Users) ปฏิบัติตามแนวทางและมาตรการในการจัดเก็บ ใช้ เปิดเผย และปกป้องข้อมูลอย่างเคร่งครัด รวมถึงรายงานเหตุการณ์ผิดปกติทันที

9.2 หน่วยงานและหน่วยงานย่อย (Data Controller and Sub-Units) กำหนดวัตถุประสงค์และขอบเขตของการประมวลผลข้อมูลส่วนบุคคล อนุมัติโครงการหรือกิจกรรมที่เกี่ยวข้อง และรับผิดชอบในการดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) สำหรับหน่วยงาน

9.3 เจ้าหน้าที่ผู้ให้บริการ (สำนักงานบริหารทรัพยากรบุคคล / สำนักทะเบียนและบริการการศึกษา / สำนักบริหารข้อมูลดิจิทัลพระจอมเกล้าเจ้าคุณทหารลาดกระบัง) ดำเนินการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (DSR) สำหรับบุคลากรและนักศึกษา กำกับดูแลการจัดเก็บและทำลายข้อมูลให้เป็นไปตามระยะเวลาการจัดเก็บข้อมูล (Retention Schedule) ที่กำหนด และจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ที่เกี่ยวข้อง

9.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) / คณะทำงานที่เกี่ยวข้อง ทำหน้าที่ให้คำปรึกษา เสนอแนะ และตรวจทานการเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) รวมถึงเป็นผู้ประสานงานและจุดเชื่อมต่อกับหน่วยงานภายนอกที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

9.5 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ (IT Administrator) / ผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Security) มีหน้าที่ดำเนินการตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านเทคนิค รวมถึงตอบสนองและจัดการต่อเหตุการณ์ละเมิดข้อมูลหรือเหตุด้านความมั่นคงปลอดภัยสารสนเทศ

10. ตัวอย่างทางปฏิบัติ

10.1 กรณีสมัครงานออนไลน์

10.1.1 ปัญหาเชิงปฏิบัติและหลักเกณฑ์ในการพิจารณาตัดสินใจ

10.1.1.1 จัดเก็บข้อมูลส่วนบุคคลเฉพาะรายการข้อมูลที่มีความจำเป็นต่อกระบวนการคัดเลือกให้สอดคล้องกับลักษณะและคุณสมบัติของตำแหน่งงาน

10.1.1.2 หลีกเลี่ยงการเก็บรวบรวมหรือร้องขอข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่จำเป็น

10.1.2 ขั้นตอนปฏิบัติ

10.1.2.1 กำหนดรายการข้อมูลที่จำเป็นในแบบฟอร์มสมัคร เช่น ชื่อ-นามสกุล หมายเลขโทรศัพท์ อีเมล ประวัติการศึกษา และประสบการณ์ที่เกี่ยวข้องกับตำแหน่งงาน พร้อมแยกรายการข้อมูลเพิ่มเติมที่ไม่จำเป็นออกเป็นข้อมูลทางเลือก

10.1.2.2 ประกาศความเป็นส่วนตัว (Privacy Notice) ให้เห็นได้อย่างชัดเจนตั้งแต่เริ่มต้นกระบวนการ หรือจัดวางไว้ใกล้ปุ่มส่งข้อมูล โดยต้องระบุรายละเอียดที่สำคัญ ได้แก่ วัตถุประสงค์ในการเก็บรวบรวมข้อมูล ระยะเวลาการจัดเก็บข้อมูล หน่วยงานหรือผู้รับผิดชอบ รวมถึงช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

10.1.2.3 จัดให้มีช่องสำหรับขอความยินยอมแยกต่างหาก กรณีมีการใช้ข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ด้านการตลาดของสถาบัน หรือการเปิดเผยข้อมูลแก่หน่วยงานภายนอก โดยการให้ความยินยอมต้องเป็นลักษณะการเลือกยินยอมโดยสมัครใจ (Opt-in) และต้องไม่มีการกำหนดเครื่องหมายยินยอมไว้ล่วงหน้า (Pre-ticked)

10.1.2.4 จำกัดสิทธิการเข้าถึงข้อมูลและผลการสรรหาเฉพาะบุคลากรสำนักงานบริหารทรัพยากรบุคคล และคณะอนุกรรมการที่เกี่ยวข้อง ตามหลักการควบคุมสิทธิการเข้าถึงตามบทบาทหน้าที่ (Role-Based Access Control: RBAC)

10.1.2.5 จัดเก็บบันทึกการเข้าถึงข้อมูลสำหรับการดาวน์โหลด การส่งต่อ หรือการเปิดดูประวัติผู้สมัครงาน (CV) รวมถึงบันทึกเหตุผลหรือวัตถุประสงค์ในการเข้าถึงข้อมูลดังกล่าว

10.1.3 ตัวอย่างข้อความโดยย่อ

10.1.3.1 **ประกาศความเป็นส่วนตัว (Privacy Notice)** “ข้อมูลส่วนบุคคลที่ท่านให้แก่สถาบันจะถูกใช้เพื่อวัตถุประสงค์ในการพิจารณาและคัดเลือกผู้สมัครงานเท่านั้น หากท่านประสงค์จะใช้สิทธิในฐานะเจ้าของข้อมูลส่วนบุคคล ต้องการข้อมูลเพิ่มเติมหรือขอให้ลบข้อมูล กรุณาติดต่อสำนักงานบริหารทรัพยากรบุคคล”

10.1.3.2 **ยินยอมการตลาด** “ข้าพเจ้ายินยอมให้สถาบันเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อการติดต่อเกี่ยวกับข้อเสนอการจ้างงาน ข่าวสาร กิจกรรมของสถาบัน และโอกาสทางอาชีพอื่นๆ”

10.1.4 ข้อควรระวัง

10.1.4.1 ห้ามส่งต่อประวัติผู้สมัครงาน (CV) ผ่านอีเมลสาธารณะ หรือแบ่งปันข้อมูลผ่านระบบจัดเก็บข้อมูลกับบุคคลภายนอก โดยไม่ได้รับความยินยอมจากผู้สมัคร

10.2 กรณีนักศึกษาสมัครทุน

10.2.1 ปัญหาเชิงปฏิบัติและหลักการตัดสินใจ

10.2.1.1 กรณีมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลด้านสุขภาพ ประวัติอาชญากรรม หรือข้อมูลเกี่ยวกับศาสนา ต้องดำเนินการขอความยินยอมเฉพาะเจาะจงจากเจ้าของข้อมูล พร้อมทั้งแจ้งรายละเอียดเกี่ยวกับวัตถุประสงค์ มาตรการรักษาความลับ และระยะเวลาในการจัดเก็บข้อมูล

10.2.2 ขั้นตอนปฏิบัติ

10.2.2.1 ประเมินความจำเป็นและความเหมาะสมก่อนดำเนินการขอข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยหากไม่มีความจำเป็นให้หลีกเลี่ยงการเก็บข้อมูลดังกล่าว

10.2.2.2 จัดทำแบบฟอร์มขอความยินยอมแยกต่างหากสำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหว

10.2.2.3 กำหนดและจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหวเฉพาะคณะกรรมการ ผู้ได้รับมอบหมาย และผู้ดูแลข้อมูล (Data Stewards) ที่ผ่านการอบรมเฉพาะด้าน

10.2.2.4 จัดเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวในพื้นที่จัดเก็บข้อมูลที่มีการเข้ารหัสลับ (Encryption) และกำหนดให้การเข้าถึงข้อมูลต้องผ่านกระบวนการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เท่านั้น

10.2.2.5 กำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวให้สั้นกว่าข้อมูลทั่วไป เช่น จัดเก็บไม่เกิน 1 ปีนับจากสิ้นสุดกระบวนการคัดเลือก และดำเนินการทำลายข้อมูลตามนโยบายที่กำหนด พร้อมจัดเก็บบันทึกการทำลายไว้เป็นหลักฐาน

10.2.3 ตัวอย่างข้อความโดยย่อ

10.2.3.1 **ขอความยินยอมเฉพาะเจาะจง (ฉบับย่อ)** “ข้าพเจ้ายินยอมให้คณะกรรมการโครงการทุนดำเนินการเก็บรวบรวมและใช้ข้อมูลด้านสุขภาพที่ระบุไว้ในใบสมัคร เพื่อวัตถุประสงค์ในการพิจารณาคัดเลือกทุนเท่านั้น โดยสถาบันจะจัดเก็บข้อมูลดังกล่าวจนถึงวันที่ 31 กุมภาพันธ์ 2569 ภายหลังครบกำหนดจะทำลายข้อมูลตามขั้นตอนของสถาบัน

10.2.4 ข้อควรระวัง

10.2.4.1 ห้ามนำข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปใช้ เปิดเผย เพื่อวัตถุประสงค์อื่น โดยไม่ได้รับความยินยอมใหม่จากเจ้าของข้อมูล

10.3 กรณีสำรองข้อมูลระบบทะเบียนนักศึกษา

10.3.1 ปัญหาเชิงปฏิบัติและหลักการตัดสินใจ

10.3.1.1 การสำรองข้อมูลของระบบทะเบียนต้องดำเนินการโดยคำนึงถึงการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมในการกู้คืนข้อมูล โดยต้องสามารถกู้คืนระบบและข้อมูลได้ตามระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) และจุดกู้คืนข้อมูล (Recovery Point Objective: RPO) ที่กำหนด

10.3.2 ขั้นตอนปฏิบัติ

10.3.2.1 กำหนดสิทธิการเข้าถึงข้อมูล Metadata และไฟล์สำรองข้อมูลอย่างชัดเจน เช่น บุคลากรฝ่ายเทคโนโลยีสารสนเทศ (IT) ตามหลักการควบคุมสิทธิการเข้าถึงตามบทบาทหน้าที่ (Role-Based Access Control: RBAC)

10.3.2.2 ดำเนินการเข้ารหัสลับไฟล์สำรองข้อมูลทั้งขณะจัดเก็บ (At Rest) และขณะรับส่งข้อมูล (In Transit) โดยใช้มาตรฐานการเข้ารหัสที่กำหนด เช่น AES-256 และจัดเก็บกุญแจเข้ารหัส แยกต่างหากในระบบบริหารจัดการกุญแจ (Key Management System: KMS)

10.3.2.3 ปฏิบัติตามหลักการสำรองข้อมูลแบบ 3-2-1 โดยจัดเก็บข้อมูลสำรองอย่างน้อย 3 ชุด บนสื่อจัดเก็บอย่างน้อย 2 ประเภท และมีอย่างน้อย 1 ชุดจัดเก็บไว้ภายนอกสถานที่ (Offisite) ซึ่งต้องมีการเข้ารหัสลับและควบคุมสิทธิการเข้าถึงอย่างเข้มงวด

10.3.2.4 จัดทำแผนการทดสอบการกู้คืนข้อมูล และดำเนินการทดสอบจริงอย่างน้อยปีละ 1 ครั้ง พร้อมจัดเก็บบันทึกขั้นตอน ผลการทดสอบ ระยะเวลาในการกู้คืนระบบและข้อมูลตามค่า RTO/RPO ที่สามารถดำเนินการได้ รวมถึงปัญหาและข้อเสนอแนะที่พบจากการทดสอบ

10.3.2.5 จัดเก็บบันทึกการเข้าถึง และการกู้คืนข้อมูลสำรองในรูปแบบบันทึกเหตุการณ์ (Log) อย่างน้อย 1 ปี

10.3.3 บันทึกที่จำเป็น

10.3.3.1 จัดทำบันทึกผลการทดสอบการกู้คืนข้อมูล โดยอย่างน้อยต้องระบุรายละเอียด ได้แก่ วันที่ดำเนินการ บริการหรือระบบที่ทำการทดสอบ ผู้รับผิดชอบหรือดำเนินการขั้นตอนการดำเนินงาน เวลาเริ่มต้นและสิ้นสุดการทดสอบ ผลการทดสอบ ปัญหาที่พบและข้อเสนอแนะเพื่อการปรับปรุง

10.3.4 ข้อควรระวัง

10.3.4.1 ห้ามจัดเก็บสำเนาสำรองข้อมูลไว้ในสื่อจัดเก็บที่ไม่มีมาตรการรักษาความมั่นคงปลอดภัย มีความเสี่ยงต่อการสูญหายง่าย หรืออาจก่อให้เกิดการเปิดเผยข้อมูลในพื้นที่สาธารณะโดยไม่ได้รับอนุญาต

10.4 กรณีการขอข้อมูลจากบุคคลภายนอกหรือหน่วยงานภายนอก

10.4.1 แนวปฏิบัติ

10.4.1.1 ตรวจสอบข้อกำหนดทางกฎหมาย ข้อตกลง และสัญญาหลัก ก่อนดำเนินการเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคลให้แก่บุคคลอื่น

10.4.1.2 ขอเอกสารเพื่อยืนยันตัวตนและเหตุผลในการขอใช้ข้อมูลส่วนบุคคลจากผู้ร้องขอข้อมูล

10.4.1.3 เปิดเผยเฉพาะข้อมูลส่วนบุคคลที่มีความจำเป็นตามคำขอ และจัดเก็บบันทึกการส่งต่อข้อมูลไว้เป็นหลักฐาน

10.4.1.4 กรณีข้อมูลส่วนบุคคลที่มีความอ่อนไหว ต้องจัดให้มีข้อตกลงการรักษาความลับ และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนดำเนินการเปิดเผยข้อมูล

10.4.2 บันทึกที่จำเป็น

10.4.2.1 จัดทำบันทึกการร้องขอข้อมูลจากภายนอก โดยอย่างน้อยต้องระบุรายละเอียด ได้แก่ ชื่อผู้ร้องขอ วันที่ดำเนินการ ขอบเขตของข้อมูล เหตุผล ผู้มีอำนาจอนุมัติ วิธีการส่งมอบข้อมูล และข้อจำกัดในการใช้ข้อมูลดังกล่าว

10.5 กรณีการเผยแพร่ข้อมูลบนเว็บไซต์หลักของสถาบัน

10.5.1 แนวปฏิบัติ

10.5.1.1 ประเมินความเสี่ยงและผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลก่อนดำเนินการเผยแพร่ข้อมูลบุคคล เช่น ภาพถ่าย ชื่อ-นามสกุล หรือผลงานของบุคคล

10.5.1.2 กรณีมีการเผยแพร่ข้อมูลของบุคลากร หรือนักศึกษา ควรเลือกใช้ข้อมูลทั่วไปแทนข้อมูลส่วนบุคคลโดยตรงเท่าที่สามารถดำเนินการได้

10.5.1.3 ในกรณีที่มีความจำเป็นต้องเผยแพร่ข้อมูลที่สามารถระบุตัวบุคคลได้ ต้องจัดให้มีการขอความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล โดยกำหนดขอบเขต วัตถุประสงค์ และระยะเวลาการเผยแพร่ข้อมูลไว้อย่างชัดเจน

10.5.2 ข้อควรระวัง

10.5.2.1 ชี้แจงช่องทางและวิธีการยกเลิกความยินยอมของเจ้าของข้อมูลส่วนบุคคล รวมถึงกำหนดกระบวนการดำเนินการนำข้อมูลออกจากการเผยแพร่ข้อมูลหลังได้รับคำร้องขออย่างชัดเจน

11. นโยบายสถาบันฯ เรื่องการคุ้มครองข้อมูลส่วนบุคคล

สาระสำคัญของนโยบาย (อ้างอิงจาก https://pdpa.kmitl.ac.th)

11.1 คำประกาศนโยบายสถาบันให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคล และมุ่งมั่นดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

11.2 ขอบเขตการบังคับใช้ นโยบายครอบคลุมการจัดเก็บข้อมูลส่วนบุคคล และประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะอยู่ในรูปแบบเอกสาร กระดาษ หรือในรูปแบบดิจิทัล

11.3 หลักการปฏิบัติ สถาบันดำเนินคุ้มครองข้อมูลส่วนบุคคลโดยยึดหลักความโปร่งใส การจำกัดสิทธิการเข้าถึงข้อมูล และรักษาความปลอดภัยข้อมูลส่วนบุคคลอย่างเหมาะสม

11.4 การกำกับดูแลและการบริหารจัดการ สถาบันกำหนดโครงสร้างการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล โดยระบุบทบาทหน้าที่ของคณะกรรมการที่เกี่ยวข้อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) รวมถึงช่องทางการแจ้งเหตุหรือรายงานกรณีข้อมูลส่วนบุคคลรั่วไหล

11.5 การดำเนินการกรณีฝ่าฝืนนโยบาย กำหนดแนวทางและมาตรการดำเนินการกรณีฝ่าฝืนหรือไม่ปฏิบัติตามนโยบาย รวมถึงการดำเนินการลงโทษทางวินัยภายในสถาบัน และตามกฎหมาย ตลอดจนการรายงานต่อหน่วยงานกำกับดูแล

ข้อปฏิบัติบุคลากรโดยย่อ

1. เข้ารับการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ตามนโยบายประจำปี

2. ใช้เฉพาะระบบที่ได้รับอนุญาตจากสถาบันในการจัดเก็บ ส่งต่อ หรือประมวลผลข้อมูลส่วนบุคคล

3. ห้ามเปิดเผย หรือเผยแพร่ข้อมูลส่วนบุคคลที่สถาบันรวบรวมไว้แก่บุคคลอื่นที่ไม่มีสิทธิ หรือไม่มีส่วนเกี่ยวข้อง

4. รายงานเหตุหรือข้อสงสัยเกี่ยวกับการรั่วไหล หรือการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือผู้รับผิดชอบของหน่วยงานโดยเร็ว

12. บทบาท หน้าที่ และสิทธิ

สิทธิพื้นฐานของเจ้าของข้อมูลส่วนบุคคล มีดังนี้

12.1 สิทธิในการเข้าถึง (Access)

12.2 สิทธิในการแก้ไข (Rectification)

12.3 สิทธิในการลบ (Erasure / Right to be forgotten)

12.4 สิทธิในการระงับ/จำกัดการประมวลผล (Restriction)

12.5 สิทธิในการคัดค้าน (Object)

12.6 สิทธิในการโอนย้ายข้อมูล (Data portability)

12.7 สิทธิในการเพิกถอนความยินยอม (Withdraw consent)

ตำแหน่ง	หน้าที่หลัก
คณะกรรมการ PDPA	กำหนดนโยบาย ทบทวนผลและอนุมัติมาตรการ
DPO/เจ้าหน้าที่ PDPA	รับคำร้อง ให้คำปรึกษา ตรวจสอบ RoPA และแจ้งเหตุการณ์
หัวหน้าหน่วยงาน	รับผิดชอบการปฏิบัติในหน่วยงาน ติดตามการทำ RoPA
เจ้าหน้าที่ปฏิบัติการ	ปฏิบัติการตามแนวทาง จัดเก็บแบบฟอร์มความยินยอม ตอบคำร้องเบื้องต้น
IT/Security	ดูแลมาตรการทางเทคนิค สำรองและเข้ารหัสข้อมูล

รายละเอียดบทบาทที่ต้องเพิ่มในการใช้งานจริง

1. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตรวจสอบกระบวนการขอความยินยอม ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และปฏิบัติหน้าที่เป็นจุดประสานงานกับหน่วยงานกำกับดูแล

2. หัวหน้าหน่วยงาน มอบหมายผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในระดับหน่วยงานย่อย เพื่อรับผิดชอบการจัดทำและทบทวนบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ของหน่วยงาน รวมถึงพิจารณาและอนุมัติการเปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานหรือบุคคลภายนอกตามอำนาจหน้าที่ที่กำหนด

13. บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: RoPA)

แบบฟอร์มบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ต้องมีการจัดทำทุกบริการ และต้องมีการทบทวน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกระบวนการดำเนินงาน ทั้งนี้ถือเป็นหลักฐานสำคัญในการแสดงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยต้องมีข้อมูลอย่างน้อยดังนี้

13.1 วันที่บันทึก/อัปเดต
13.2 หน่วยงาน/หน่วยงานย่อย
13.3 ผู้รับผิดชอบ (ชื่อ/ตำแหน่ง/อีเมล)
13.4 ชื่อกระบวนการ/ระบบ/บริการ
13.5 วัตถุประสงค์การประมวลผล
13.6 ประเภทของเจ้าของข้อมูล
13.7 ประเภทข้อมูลที่ประมวลผล
13.8 แหล่งที่มาของข้อมูล (เจ้าของข้อมูล/บุคคลที่สาม)
13.9 ผู้รับ/ผู้ถูกเปิดเผยข้อมูล (ภายใน/ภายนอก)
13.10 ระยะเวลาเก็บรักษา
13.11 ฐานกฎหมายสำหรับการประมวลผล
13.12 มาตรการความปลอดภัยที่ใช้งาน
13.13 การโอนข้อมูลข้ามประเทศ
13.14 การประเมินความเสี่ยงและมาตรการบรรเทา

ตัวอย่าง RoPA ระบบจ่ายเงินเดือน

ฟิลด์	รายละเอียด
หน่วยงาน	สำนักบริหารทรัพยากรบุคคล
ผู้รับผิดชอบ	Mr. Lorem Ipsum (lorem@kmitl.a.cth)
ชื่อระบบ	ระบบเงินเดือนภายใน
วัตถุประสงค์	จ่ายเงินเดือนและปฏิบัติตามภาษีและสวัสดิการ
วันที่อัปเดต	31 ก.พ. 2569
ประเภทเจ้าของข้อมูล	พนักงานประจำ, พนักงานชั่วคราว
ประเภทข้อมูล	ชื่อ, เลขบัตรประชาชน, เลขบัญชีธนาคาร, รายได้, ภาษี
แหล่งที่มาของข้อมูล	เจ้าของข้อมูล/เอกสารสมัคร/หน่วยงานภายใน
ผู้รับข้อมูล	ฝ่ายบัญชี, ธนาคาร, หน่วยงานภาษี
ระยะเวลาเก็บรักษา	สิ้นสุดการจ้าง + 10 ปี
ฐานกฎหมาย	สัญญาจ้าง, กฎหมายแรงงาน, กฎหมายภาษี
มาตรการความปลอดภัย	เข้ารหัสฐานข้อมูล, MFA, จำกัดสิทธิบนระบบ
โอนข้ามประเทศ	ไม่มี
การประเมินความเสี่ยง	ความเสี่ยงรั่วไหลทางอีเมล (มาตรการ: เข้ารหัสลับอีเมลหรือใช้พอร์ทัลส่งไฟล์แทน)

14. ตารางระยะเวลาการเก็บรักษาข้อมูล (Retention Schedule)

ตัวอย่างสำหรับ สำนักงานบริหารทรัพยากรบุคคล

ประเภทเอกสาร	ระยะเวลาจัดเก็บ	เหตุผลทางกฎหมาย/ข้อปฏิบัติ
ใบสมัครงาน และ CV	6 เดือน หลังสิ้นสุดการคัดเลือก	เก็บเป็นหลักฐานการสรรหา
สัญญาจ้าง	สิ้นสุดการจ้าง + 10 ปี	ภาษี/แรงงาน
บันทึกการลา / ใบรับรองแพทย์	5 ปี	หลักฐานการลางาน
เอกสารเงินเดือน / ใบหักภาษี	10 ปี	ภาษีและบัญชี
ข้อมูลสุขภาพที่เกี่ยวข้องกับงาน	เท่าที่จำเป็น; ระบุใน RoPA	ข้อมูลอ่อนไหว — ต้องมีมาตรการพิเศษ

ตัวอย่างสำหรับ สำนักทะเบียน และบริการการศึกษา

ประเภทเอกสาร	ระยะเวลาจัดเก็บ	เหตุผลทางกฎหมาย/ข้อปฏิบัติ
ใบสมัครเข้าเรียน (ผู้ไม่สำเร็จ)	5 ปี หลังปีที่สมัคร	เก็บเป็นหลักฐานการรับสมัคร
ทรานสคริปต์ ผลการเรียน	เก็บถาวร	ประวัติการศึกษาของนักศึกษา
ประกาศนียบัตร	เก็บถาวร	เอกสารทางการศึกษา
บันทึกวินัย	5-15 ปี (ตามความรุนแรง)	ขึ้นกับนโยบายภายใน
ข้อมูลการฉีดวัคซีน	เท่าที่จำเป็นและตามวัตถุประสงค์	ต้องมีความยินยอมหรือฐานกฎหมาย

แนวทางปฏิบัติ

1. ควรกำหนดวิธีการทำลายข้อมูลและระบุผู้รับผิดชอบให้ชัดเจนภายในตาราง

2. ควรระบุฐานกฎหมายสำหรับเอกสารแต่ละประเภทไว้ในตารางกำหนดระยะเวลาการจัดเก็บข้อมูล (Retention Schedule) อย่างครบถ้วน

15. ตัวอย่างปัญหาและแนวทางบรรเทา

15.1 กรณีศึกษา: สำนักงานบริหารทรัพยากรบุคคลส่งรายการโอนเงินเดือนทางอีเมลให้แก่ธนาคาร

15.1.1 ประเด็นปัญหา ส่งไฟล์ Microsoft Excel ที่มีหมายเลขบัตรประจำตัวประชาชนและข้อมูลรายได้ผ่านอีเมลทั่วไปไปยังธนาคาร

15.1.2 ผลกระทบที่อาจเกิดขึ้น อาจก่อให้เกิดความเสี่ยงต่อการรั่วไหลข้อมูลส่วนบุคคลที่อ่อนไหว

15.1.3 แนวทางการแก้ไข ควรใช้พอร์ทัลสำหรับการจัดการข้อมูลเงินเดือนที่มีมาตรการการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) รวมถึงจัดส่งไฟล์ข้อมูลในรูปแบบที่มีการเข้ารหัสลับ

15.2 กรณีศึกษา: สำนักทะเบียนและบริการการศึกษา มีการเผยแพร่รายชื่อนักศึกษาและคะแนนผลการเรียนผ่านหน้าเว็บไซต์

15.2.1 ประเด็นปัญหา มีการเผยแพร่รายชื่อนักศึกษาและคะแนนผลการเรียนผ่านหน้าเว็บไซต์ของสำนักทะเบียนและบริการการศึกษา

15.2.2 ผลกระทบที่อาจเกิดขึ้น อาจเข้าข่ายการละเมิดความเป็นส่วนตัว และอาจก่อให้เกิดผลกระทบต่อเจ้าของข้อมูล

15.2.3 แนวทางการแก้ไข ควรใช้รหัสประจำตัวนักศึกษาแทนการแสดงชื่อ-นามสกุล และกำหนดสิทธิการเข้าถึงข้อมูลเฉพาะผู้สอนหรือผู้มีส่วนได้ส่วนเสีย