

-ร่าง- นโยบายการกำกับดูแลข้อมูล (Data Governance Policy)

1. วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการบริหารจัดการข้อมูลของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล ให้เป็นไปตามมาตรฐานสากลและกฎหมายที่เกี่ยวข้อง โดยมุ่งเน้นการรักษาความปลอดภัย ความเป็นส่วนตัว และความถูกต้องของข้อมูล เพื่อสนับสนุนการดำเนินงานของคณะอย่างมีประสิทธิภาพ

2. ขอบเขต

นโยบายนี้ครอบคลุมข้อมูลทุกประเภทที่จัดเก็บ ใช้งาน และเผยแพร่ภายในคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล รวมถึงบุคลากรที่เกี่ยวข้องทุกระดับ

3. การปฏิบัติตามกฎหมายและมาตรฐาน

3.1 ปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มาตรา 37 และ 38 ที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล เพื่อป้องกันการละเมิดสิทธิของเจ้าของข้อมูล

3.2 ปฏิบัติตามมาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานความมั่นคงปลอดภัยของข้อมูล เพื่อบริหารจัดการความเสี่ยงด้านข้อมูล

3.3 ปฏิบัติตาม มาตรฐาน ISO/IEC 27701 สำหรับการบริหารจัดการข้อมูลส่วนบุคคล (Privacy Information Management System - PIMS)

3.4 ปฏิบัติตาม ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งกำหนดแนวทางการจัดระดับข้อมูลเพื่อรักษาความปลอดภัยของข้อมูลภาครัฐ

4. การควบคุมการเข้าถึงข้อมูล

4.1 ใช้หลักการ Least Privilege โดยให้สิทธิ์การเข้าถึงข้อมูลเฉพาะบุคลากรที่จำเป็นต้องใช้เท่านั้น

4.2 ใช้ระบบ Role-Based Access Control (RBAC) กำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่

4.3 ปฏิบัติตาม แนวทางการบริหารจัดการข้อมูลของภาครัฐ ตามนโยบายดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เพื่อควบคุมและปกป้องข้อมูลของหน่วยงาน

5. มาตรการรักษาความปลอดภัยของข้อมูล

5.1 ใช้ การเข้ารหัสข้อมูล (Data Encryption) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5.2 บันทึกและตรวจสอบ Audit Logging เพื่อระบุและติดตามกิจกรรมที่เกี่ยวข้องกับข้อมูล

5.3 ใช้ **Data Masking และ Anonymization** สำหรับข้อมูลที่อ่อนไหวเพื่อป้องกันการเปิดเผยข้อมูลส่วนบุคคลโดยไม่จำเป็น

6. การจัดการข้อมูล

6.1 จัดประเภทข้อมูลตามระดับความสำคัญและความอ่อนไหว (**Data Classification**) เพื่อกำหนดมาตรการป้องกันที่เหมาะสม

6.2 กำหนด **Data Retention Policy** ระบุระยะเวลาในการเก็บรักษาและลบข้อมูลตามความจำเป็นและกฎหมายที่เกี่ยวข้อง

6.3 ปฏิบัติตามแนวทาง **Data Integrity and Accuracy** เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องและเชื่อถือได้

7. การบังคับใช้และการตรวจสอบ

7.1 มีการอบรมบุคลากรเกี่ยวกับนโยบายการกำกับดูแลข้อมูลอย่างสม่ำเสมอ

7.2 ดำเนินการตรวจสอบการปฏิบัติตามนโยบายเป็นระยะ และปรับปรุงนโยบายให้ทันสมัยตามความเหมาะสม

7.3 มีมาตรการลงโทษทางวินัยหากมีการละเมิดนโยบาย ตามกฎหมายและระเบียบของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล

การละเมิดนโยบายนี้อาจนำไปสู่มาตรการทางวินัยตามระเบียบของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล และกฎหมายที่เกี่ยวข้อง