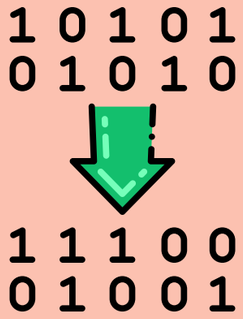
มาตรการรักษาความปลอดภัย ข้อมูลส่วนบุคคล

Anonymization

การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หากสามารถทำได้โดยไม่ทำให้เสียวัตถุประสงค์ในการวิจัยหรือสถิติ



Pseudonymization

การใช้รหัสอ้างอิงแทนการใช้ชื่อหรือข้อมูลส่วนบุคคล ในการวิเคราะห์ข้อมูล หากไม่มีความจำเป็นต้องระบุตัวบุคคลในขั้นตอนนั้น

Encryption

การเข้ารหัสข้อมูลที่จัดเก็บอยู่ในอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

Access Control

การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและระบบสารสนเทศที่สำคัญ ที่มีการพิสูจน์และยืนยันตัวตน (Authentication) เท่าที่จำเป็น ตลอดจนการทบทวนสิทธิ์ในการเข้าถึงและใช้งานของผู้เกี่ยวข้องเป็นระยะ

User Responsibities

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานที่เกี่ยวข้อง เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงการกระทำนอกเหนือบทบาทที่ได้รับมอบหมาย

Privacy and Security Awareness

การสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมให้ผู้เกี่ยวข้องทราบและถือปฏิบัติ

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

การใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีการปรับปรุงให้เป็นปัจจุบัน การใช้งานโปรแกรมป้องกันไวรัส (Antivirus Software) การระมัดระวังภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ

Physical Security

การรักษาความมั่งคงปลอดภัยทางกายภาพ เพื่อให้ข้อมูลส่วนบุคคลในรูปแบบเอกสาร ตลอดจนอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลมีความมั่นคงปลอดภัยตามสมควร

Data Backup

การสำรองข้อมูลที่สำคัญไว้ในที่ปลอดภัย

จัดทำโดย: คณะทำงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล สถาบันนวัตกรรมการเรียนรู้

ที่มา: ประกาศมหาวิทยาลัยมหิดล เรื่อง แนวปฏิบัติและมาตรการสำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อการวิจัยและสถิติ พ.ศ.2567