

แนวทางปฏิบัติสำหรับการปกปิดข้อมูลส่วนบุคคล

แนวทางปฏิบัติสำหรับการปกปิดข้อมูลส่วนบุคคล (Personal Data Masking)

บทนำ

แนวทางปฏิบัติในการปกปิดข้อมูลส่วนบุคคล (Personal Data Masking) ฉบับนี้ เป็นวิธีการปกปิดข้อมูลส่วนบุคคล เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลที่ไม่พึงประสงค์จากผู้ที่ไม่มีความจำเป็นและรักษาความปลอดภัยข้อมูลส่วนบุคคล โดยไม่ต้องลบข้อมูลส่วนบุคคลออกจากภาวะ

วัตถุประสงค์ของการทำ Personal Data Masking

1. เพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล : ป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกเข้าถึงหรือใช้งาน โดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำข้อมูลส่วนบุคคลไปใช้ในการโฆษณาหรือกิจกรรม
2. เพื่อลดความเสี่ยงในการเปิดเผยข้อมูล : ลดความเสี่ยงจากการเปิดเผยข้อมูล โดยไม่ได้ตั้งใจหรือจากข้อผิดพลาดที่อาจเกิดขึ้นในการจัดการข้อมูล
3. เพื่อปฏิบัติตามข้อกำหนดทางกฎหมาย : ปฏิบัติให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการมอบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567

กระบวนการปกปิดข้อมูลส่วนบุคคล (Personal Data Masking Process)

1. ระบุประเภทของข้อมูลส่วนบุคคลที่ต้องการปกปิด: ระบุข้อมูลส่วนบุคคลที่ต้องการปกปิดว่าเป็นข้อมูลส่วนบุคคลประเภทใด เช่น ข้อมูลส่วนบุคคลของพนักงาน ข้อมูลส่วนบุคคลของลูกค้า ข้อมูลส่วนบุคคลของผู้ถือหุ้นและนักลงทุน
2. ประเมินการปกปิดข้อมูลส่วนบุคคล: ประเมินการปกปิดข้อมูลส่วนบุคคลแต่ละวิธี เช่น การปกปิดข้อมูลบางส่วน การลบข้อมูล การเข้ารหัสข้อมูล การแทนที่ข้อมูลส่วนบุคคลเทียม การเปลี่ยนข้อมูลให้เป็นข้อมูลทั่วไป ไม่ว่าการปกปิดข้อมูลส่วนบุคคลแต่ละวิธีมีผลกระทบอะไรบ้างและมีความเหมาะสมอย่างไร
3. เลือกวิธีการปกปิดข้อมูลส่วนบุคคลที่เหมาะสม
4. ควบคุมการเข้าถึง : กำหนดและจัดการสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกปกปิดอย่างเคร่งครัด เพื่อป้องกันไม่ให้ข้อมูลถูกเปิดเผย
5. ตรวจสอบและปรับปรุงวิธีการปกปิดข้อมูล: ตรวจสอบและปรับปรุงวิธี Personal Data Masking อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าวิธีการปกปิดข้อมูลส่วนบุคคลได้นั้นยังคงมีประสิทธิภาพและความปลอดภัย
6. ให้ความรู้และอบรม: ให้ความรู้และฝึกอบรมแก่พนักงานหรือผู้ที่เกี่ยวข้องเกี่ยวกับการปกปิดข้อมูลส่วนบุคคล (Personal Data Masking) เพื่อให้เข้าใจและสามารถปฏิบัติตามแนวทางได้อย่างถูกต้อง

Employee Personal Data Masking

วิธีการและตัวอย่างของ Employee Personal Data Masking

1. การปกปิดข้อมูลบางส่วน:

- ชื่อ: ปิดบังชื่อนามสกุล เหลือเพียงชื่อย่อ เช่น นาย ส. หรือ นางสาว ด.
- เลขประจำตัวประชาชน: ปิดบังตัวเลขบางส่วน เช่น 3-1001-XXXX-567-8
- บ้านเลขที่: หมายเลขของบ้านเลขที่ให้เหลืออยู่บางส่วน เช่น 1XX/1X
- บัญชีธนาคาร: ปิดบังตัวเลขบางส่วนออก เช่น 2000-X-XXXX-X

- เบอร์โทรศัพท์: ปิดบังตัวเลขบางส่วน เช่น 081-XXXX-XXXX
- ที่อยู่ผู้มีเมล: เปลี่ยนโดเมนอีเมล เช่น tinbobdee@mfec.co.th เป็น tinbobdee@xyz.com
- วันเกิด: ปิดบังปีเกิด เหลือเพียงเดือนและวันเกิด เช่น 14/02/XX
- หมายเลขรหัสสมาชิก: จากตัวอย่าง 1234-5678-9012 เป็น XXXX-XXXX-9012 แสดงตัวเลข 4 หลักสุดท้าย
- หมายเลขทะเบียนรถ: จากตัวอย่าง ABC-1234 เป็น XXX-1234
ปิดบังตัวอักษรแต่ยังคงแสดงตัวเลข 4 หลักสุดท้าย
- ภาพใบหน้า: ทำการเบลอภาพใบหน้าหรือใช้เทคนิคในการครอบคลุมส่วนของใบหน้า เช่น การใช้ Pixelation หรือ Gaussian Blur ปิดบังใบหน้าเพื่อให้ไม่สามารถระบุตัวตนได้ แต่ยังสามารถมองเห็นภาพรวมของบุคคล
- ข้อมูลชีวภาพ: เช่น ลายนิ้วมือ หรือการจดจำใบหน้า ควรถูกเข้ารหัส (Encryption) หรือถูกทำให้เป็นนิรนาม (Anonymization)
- รหัสบัญชีผู้ใช้งาน: จากตัวอย่าง user1234 เป็น uXXX1234 หรือ UXXXXXX
- แสดงเฉพาะตัวอักษรหรือตัวเลขบางส่วน ส่วนที่เหลือจะถูกปิดบังด้วย X หรือ *

2. การสุ่มข้อมูล:

- ชื่อ: สุ่มชื่อใหม่จากฐานข้อมูลทั่วไป
- เลขประจำตัวประชาชน: สุ่มเลขประจำตัวประชาชนใหม่ แต่ต้องไม่ซ้ำกับเลขประจำตัวประชาชนจริง
- บ้านเลขที่: สุ่มบ้านเลขที่ใหม่ แต่ต้องไม่ซ้ำกับบ้านเลขที่จริง
- บัญชีธนาคาร: สุ่มบัญชีธนาคารใหม่ แต่ต้องไม่ซ้ำกับบัญชีธนาคารจริง
- เบอร์โทรศัพท์: สุ่มเบอร์โทรศัพท์ใหม่ แต่ต้องไม่ซ้ำกับเบอร์โทรศัพท์จริง
- ที่อยู่ผู้มีเมล: สุ่มโดเมนอีเมลใหม่
- วันเกิด: สุ่มวันเกิดใหม่
- หมายเลขรหัสสมาชิก: สุ่มรหัสสมาชิกใหม่
- หมายเลขทะเบียนรถ: สุ่มทะเบียนรถใหม่
- ภาพใบหน้า: นำเสนอภาพการ์ตูน หรือภาพที่อยู่ในคลังรูปภาพที่ไม่ใช่เจ้าของข้อมูลสารสนเทศ
- ข้อมูลชีวภาพ: สุ่มข้อมูลชีวภาพ
- รหัสบัญชีผู้ใช้งาน: สุ่มบัญชีผู้ใช้งานใหม่

3. การเข้ารหัสข้อมูล:

- ชื่อ: เข้ารหัสชื่อด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- เลขประจำตัวประชาชน: เข้ารหัสเลขประจำตัวประชาชนด้วยอัลกอริทึมการเข้ารหัส
- เบอร์โทรศัพท์: เข้ารหัสเบอร์โทรศัพท์ด้วยอัลกอริทึมการเข้ารหัส
- บ้านเลขที่: เข้ารหัสบ้านเลขที่ด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- บัญชีธนาคาร: เข้ารหัสบัญชีธนาคารด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- เลขที่ประกันสังคม: เข้ารหัสเลขที่ประกันสังคมด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- ที่อยู่ผู้มีเมล: เข้ารหัสที่อยู่ผู้มีเมลด้วยอัลกอริทึมการเข้ารหัส
- วันเกิด: เข้ารหัสวันเกิดด้วยอัลกอริทึมการเข้ารหัส
- หมายเลขรหัสสมาชิก: เข้ารหัสหมายเลขสมาชิกด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

- **หมายเลขทะเบียนรถ:** เข้ารหัสหมายเลขทะเบียนรถด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **ภาพใบหน้า:** เข้ารหัสข้อมูลภาพใบหน้าด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **ข้อมูลชีวภาพ:** เข้ารหัสข้อมูลชีวภาพด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **รหัสบัญชีผู้ใช้งาน:** เข้ารหัสรหัสบัญชีผู้ใช้งานด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

4. การใช้เทคนิคอื่น ๆ:

- **การใช้ Pseudonymization:** แทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลเทียม เช่น แทนชื่อ "สมชาย" ด้วย "A001"
- **การใช้ Generalization:** เปลี่ยนข้อมูลให้เป็นข้อมูลทั่วไป เช่น แทนที่ "กรุงเทพมหานคร" ด้วย "ภาคกลาง"

ข้อควรระวัง:

- **Data Masking** ไม่ได้ลบข้อมูลส่วนบุคคลออกถาวร ข้อมูลที่ถูกปกปิดอาจถูกกู้คืนได้โดยผู้เชี่ยวชาญ
- **Data Masking** ควรดำเนินการโดยคำนึงถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
- ควรมีมาตรการป้องกันข้อมูลที่เกี่ยวข้อง เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึงข้อมูล

Vendor/Supplier Personal Data Masking วิธีการและตัวอย่างของ Vendor/Supplier Personal Data Masking

1. การปกปิดข้อมูลบางส่วน:

- **ชื่อบริษัท:** ปิดบังชื่อบริษัท เหลือเพียงชื่อย่อ เช่น บจ. ส. หรือ บจก. ต.
- **เลขประจำตัวผู้เสียภาษี:** ปิดบังตัวเลขบางส่วน เช่น 01236-XXXX-XXXX-XXXX
- **บัญชีธนาคาร:** ปิดบังตัวเลขบางส่วนออก เช่น 2000-X-XXXX-X
- **เบอร์โทรศัพท์:** ปิดบังตัวเลขบางส่วน เช่น 02-XXXX-XXXX
- **ที่อยู่ผู้มีอีเมล:** เปลี่ยนโดเมนอีเมล เช่น [อีเมลถูกนำออกแล้ว] เป็น [อีเมลถูกนำออกแล้ว]
- **เว็บไซต์:** เปลี่ยน URL เว็บไซต์
- **หมายเลขรหัสสมาชิก:** จากตัวอย่าง 1234-5678-9012 เป็น XXXX-XXXX-9012 แสดงตัวเลข 4 หลักสุดท้าย
- **หมายเลขทะเบียนรถ:** จากตัวอย่าง ABC-1234 เป็น XXX-1234 ปิดบังตัวอักษรแต่ยังคงแสดงตัวเลข 4 หลักสุดท้าย
- **ภาพใบหน้า:** ทำการเบลภาพใบหน้าหรือใช้เทคนิคในการครอบคลุมส่วนของใบหน้า เช่น การใช้ Pixelation หรือ Gaussian Blur ปิดบังใบหน้าเพื่อให้ไม่สามารถระบุตัวตนได้ แต่ยังสามารถมองเห็นภาพรวมของบุคคล
- **ข้อมูลชีวภาพ:** เช่น ลายนิ้วมือ หรือการจดจำใบหน้า ควรถูกเข้ารหัส (Encryption) หรือถูกทำให้เป็นนิรนาม (Anonymization)
- **รหัสบัญชีผู้ใช้งาน:** จากตัวอย่าง user1234 เป็น uXXX1234 หรือ UXXXXXX แสดงเฉพาะตัวอักษรหรือตัวเลขบางส่วน ส่วนที่เหลือจะถูกปิดบังด้วย X หรือ *

2. การสุ่มข้อมูล:

- **ชื่อบริษัท:** สุ่มชื่อบริษัทใหม่จากฐานข้อมูลบริษัททั่วไป
- **เลขประจำตัวผู้เสียภาษี:** สุ่มเลขประจำตัวผู้เสียภาษีใหม่ แต่ต้องไม่ซ้ำกับเลขประจำตัวผู้เสียภาษีจริง
- **บัญชีธนาคาร:** สุ่มบัญชีธนาคารใหม่ แต่ต้องไม่ซ้ำกับบัญชีธนาคารจริง
- **เบอร์โทรศัพท์:** สุ่มเบอร์โทรศัพท์ใหม่ แต่ต้องไม่ซ้ำกับเบอร์โทรศัพท์จริง
- **ที่อยู่ผู้มีอีเมล:** สุ่ม โดเมนอีเมลใหม่

- เว็บไซต์: กลุ่ม URL เว็บไซต์ใหม่
- หมายเลขรหัสสมาชิก: กลุ่มรหัสสมาชิกใหม่
- หมายเลขทะเบียนรถ: กลุ่มทะเบียนรถใหม่
- ภาพใบหน้า: นำเสนอภาพการ์ตูน หรือภาพที่อยู่ในคลังรูปภาพที่ไม่ใช่เจ้าของข้อมูลสารสนเทศ
- ข้อมูลชีวภาพ: กลุ่มข้อมูลชีวภาพ
- รหัสบัญชีผู้ใช้งาน: กลุ่มบัญชีผู้ใช้งานใหม่

3. การเข้ารหัสข้อมูล:

ข้อปฏิบัติ: เข้ารหัสข้อมูลด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

- เลขประจำตัวผู้เสียภาษี: เข้ารหัสเลขประจำตัวผู้เสียภาษีด้วยอัลกอริทึมการเข้ารหัส
- บัญชีธนาคาร: เข้ารหัสบัญชีธนาคารด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- เบอร์โทรศัพท์: เข้ารหัสเบอร์โทรศัพท์ด้วยอัลกอริทึมการเข้ารหัส
- ที่อยู่ผู้มีมรดก: เข้ารหัสที่อยู่ผู้มีมรดกด้วยอัลกอริทึมการเข้ารหัส
- เว็บไซต์: เข้ารหัส URL เว็บไซต์ด้วยอัลกอริทึมการเข้ารหัส
- หมายเลขรหัสสมาชิก: เข้ารหัสหมายเลขสมาชิกด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- หมายเลขทะเบียนรถ: เข้ารหัสหมายเลขทะเบียนรถด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- ภาพใบหน้า: เข้ารหัสข้อมูลภาพใบหน้าด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- ข้อมูลชีวภาพ: เข้ารหัสข้อมูลชีวภาพด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- รหัสบัญชีผู้ใช้งาน: เข้ารหัสรหัสบัญชีผู้ใช้งานด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

4. การใช้เทคนิคอื่น ๆ:

- การใช้ Pseudonymization: แทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลเทียม เช่น แทนชื่อ "บริษัท ABC" ด้วย "C001"
- การใช้ Generalization: เปลี่ยนข้อมูลให้เป็นข้อมูลทั่วไป เช่น แทนที่ "กรุงเทพมหานคร" ด้วย "ภาคกลาง"

ข้อควรระวัง:

- Data Masking ไม่ได้ลบข้อมูลส่วนบุคคลออกถาวร ข้อมูลที่ถูกปกปิดอาจถูกกู้คืนได้โดยผู้เชี่ยวชาญ
- Data Masking ควรดำเนินการโดยคำนึงถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
- ควรมีมาตรการป้องกันข้อมูลที่เพียงพอ เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึงข้อมูล

Customer Personal Data Masking วิธีการและตัวอย่างของ Customer Personal Data Masking

1. การปกปิดข้อมูลบางส่วน:

- ชื่อ: ปิดบังชื่อนามสกุล เหลือเพียงชื่อย่อ เช่น นาย ค. หรือ นางสาว ค.
- เลขประจำตัวประชาชน: ปิดบังตัวเลขบางส่วน เช่น 12-3XXX-XXXX-23-4
- เลขหนังสือเดินทาง: ปิดบังตัวเลขบางส่วน เช่น 2000-XXXX-XXXX
- ชื่อและรหัสผ่านเข้าใช้ระบบ: ปิดบังชื่อชื่อนามสกุลออกและรหัสผ่านให้แสดงเป็น *****
- เบอร์โทรศัพท์: ปิดบังตัวเลขบางส่วน เช่น 081-XXXX-XXXX
- ที่อยู่ผู้มีมรดก: เปลี่ยนโดเมนอีเมล เช่น [อีเมลถูกนำออกแล้ว] เป็น [อีเมลถูกนำออกแล้ว]
- ที่อยู่: ปิดบังรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน

- **วันเกิด:** ปิดบังปีเกิด เหลือเพียงเดือนและวันเกิด
- **หมายเลขรหัสสมาชิก:** จากตัวอย่าง 1234-5678-9012 เป็น XXXX-XXXX-9012 แสดงตัวเลข 4 หลักสุดท้าย
- **หมายเลขทะเบียนรถ:** จากตัวอย่าง ABC-1234 เป็น XXX-1234 ปิดบังตัวอักษรแต่ยังคงแสดงตัวเลข 4 หลักสุดท้าย
- **ภาพใบหน้า:** ทำการเบลอภาพใบหน้าหรือใช้เทคนิคในการครอบคลุมส่วนของใบหน้า เช่น การใช้ Pixelation หรือ Gaussian Blur ปิดบังใบหน้าเพื่อให้ไม่สามารถระบุตัวตนได้ แต่ยังสามารถมองเห็นภาพรวมของบุคคล
- **ข้อมูลชีวภาพ:** เช่น ลายนิ้วมือ หรือการจดจำใบหน้า ควรถูกเข้ารหัส (Encryption) หรือถูกทำให้เป็นนิรนาม (Anonymization)
- **รหัสบัญชีผู้ใช้งาน:** จากตัวอย่าง user1234 เป็น uXXX1234 หรือ UXXXXXX แสดงเฉพาะตัวอักษรหรือตัวเลขบางส่วน ส่วนที่เหลือจะถูกปิดบังด้วย X หรือ *

2. การคุ้มครองข้อมูล:

- **ชื่อ:** คู่สมชื่อใหม่จากฐานข้อมูลทั่วไป
- **เลขประจำตัวประชาชน:** คู่สมเลขประจำตัวประชาชนใหม่ แต่ต้องไม่ซ้ำกับเลขประจำตัวประชาชนจริง
- **เลขหนังสือเดินทาง:** คู่สมเลขหนังสือเดินทางใหม่ แต่ต้องไม่ซ้ำกับเลขหนังสือเดินทางจริง
- **ชื่อและรหัสผ่านเข้าใช้ระบบ:** คู่สมชื่อใหม่จากฐานข้อมูล และซ่อนรหัสผ่านด้วย *****
- **เบอร์โทรศัพท์:** คู่สมเบอร์โทรศัพท์ใหม่ แต่ต้องไม่ซ้ำกับเบอร์โทรศัพท์จริง
- **ที่อยู่ผู้มีเมล:** คู่สมโดเมนอีเมลใหม่
- **ที่อยู่:** คู่สมรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- **วันเกิด:** คู่สมวันเกิดใหม่
- **หมายเลขรหัสสมาชิก:** คู่สมรหัสสมาชิกใหม่
- **หมายเลขทะเบียนรถ:** คู่สมทะเบียนรถใหม่
- **ภาพใบหน้า:** นำเสนอภาพการ์ตูน หรือภาพที่อยู่ในคลังรูปภาพที่ไม่ใช่เจ้าของข้อมูลสารสนเทศ
- **ข้อมูลชีวภาพ:** คู่สมข้อมูลชีวภาพ
- **รหัสบัญชีผู้ใช้งาน:** คู่สมบัญชีผู้ใช้งานใหม่

3. การเข้ารหัสข้อมูล:

- **ชื่อ:** เข้ารหัสชื่อด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **เลขประจำตัวประชาชน:** เข้ารหัสเลขประจำตัวประชาชนด้วยอัลกอริทึมการเข้ารหัส
- **เลขหนังสือเดินทาง:** เข้ารหัสเลขหนังสือเดินทางด้วยอัลกอริทึมการเข้ารหัส
- **ชื่อและรหัสผ่านเข้าใช้ระบบ:** เข้ารหัสชื่อและรหัสผ่านด้วยอัลกอริทึมการเข้ารหัส
- **เบอร์โทรศัพท์:** เข้ารหัสเบอร์โทรศัพท์ด้วยอัลกอริทึมการเข้ารหัส
- **ที่อยู่ผู้มีเมล:** เข้ารหัสที่อยู่ผู้มีเมลด้วยอัลกอริทึมการเข้ารหัส
- **ที่อยู่:** เข้ารหัสรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- **วันเกิด:** เข้ารหัสวันเกิดด้วยอัลกอริทึมการเข้ารหัส
- **หมายเลขรหัสสมาชิก:** เข้ารหัสหมายเลขสมาชิกด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **หมายเลขทะเบียนรถ:** เข้ารหัสหมายเลขทะเบียนรถด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

- ภาพใบหน้า: เข้ารหัสข้อมูลภาพใบหน้าด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- ข้อมูลชีวภาพ: เข้ารหัสข้อมูลชีวภาพด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- รหัสบัญชีผู้ใช้งาน: เข้ารหัสรหัสบัญชีผู้ใช้งานด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

4. การใช้เทคนิคอื่น ๆ:

- การใช้ Pseudonymization: แทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลเทียม เช่น แทนชื่อ "สมชาย" ด้วย "A001"
- การใช้ Generalization: เปลี่ยนข้อมูลให้เป็นข้อมูลทั่วไป เช่น แทนที่ "กรุงเทพมหานคร" ด้วย "ภาคกลาง"

ข้อควรระวัง:

- Data Masking ไม่ได้ลบข้อมูลส่วนบุคคลออกถาวร ข้อมูลที่ถูกปกปิดอาจถูกกู้คืนได้โดยผู้เชี่ยวชาญ
- Data Masking ควรดำเนินการโดยคำนึงถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
- ควรมีมาตรการป้องกันข้อมูลที่เพียงพอ เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึงข้อมูล

Applicant Personal Data Masking

วิธีการและตัวอย่างของ Applicant Personal Data Masking

1. การปกปิดข้อมูลบางส่วน:

- ชื่อ: ปิดบังชื่อนามสกุล เหลือเพียงชื่อย่อ เช่น นาย ต. หรือ นางสาว ด.
- เลขประจำตัวประชาชน: ปิดบังตัวเลขบางส่วน เช่น 12-3XXX-XXXX-23-4
- เบอร์โทรศัพท์: ปิดบังตัวเลขบางส่วน เช่น 081-XXXX-XXXX
- ที่อยู่ผู้มีเมล: เปลี่ยนโดเมนอีเมล เช่น [อีเมลถูกนำออกแล้ว] เป็น [อีเมลถูกนำออกแล้ว]
- ที่อยู่: ปิดบังรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- วันเกิด: ปิดบังปีเกิด เหลือเพียงเดือนและวันเกิด
- ข้อมูลการศึกษา: ปิดบังชื่อสถานศึกษาเหลือเพียงระดับการศึกษา
- ประสบการณ์การทำงาน: ปิดบังชื่อบริษัทเหลือเพียงตำแหน่งงานและระยะเวลาการทำงาน
- ภาพใบหน้า: ทำการเบลภาพใบหน้าหรือใช้เทคนิคในการครอบคลุมส่วนของใบหน้า เช่น การใช้ Pixelation หรือ Gaussian Blur ปิดบังใบหน้าเพื่อให้ไม่สามารถระบุตัวตนได้ แต่ยังสามารถมองเห็นภาพรวมของบุคคล
- ข้อมูลชีวภาพ: เช่น ลายนิ้วมือ หรือการจดจำใบหน้า ควรถูกเข้ารหัส (Encryption) หรือถูกทำให้เป็นนิรนาม (Anonymization)
- รหัสบัญชีผู้ใช้งาน: จากตัวอย่าง user1234 เป็น uXXX1234 หรือ UXXXXXX แสดงเฉพาะตัวอักษรหรือตัวเลขบางส่วน ส่วนที่เหลือจะถูกปิดบังด้วย X หรือ *

2. การสุ่มข้อมูล:

- ชื่อ: สุ่มชื่อใหม่จากฐานข้อมูลทั่วไป
- เลขประจำตัวประชาชน: สุ่มเลขประจำตัวประชาชนใหม่ แต่ต้องไม่ซ้ำกับเลขประจำตัวประชาชนจริง
- เบอร์โทรศัพท์: สุ่มเบอร์โทรศัพท์ใหม่ แต่ต้องไม่ซ้ำกับเบอร์โทรศัพท์จริง
- ที่อยู่ผู้มีเมล: สุ่มโดเมนอีเมลใหม่
- ที่อยู่: สุ่มรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- วันเกิด: สุ่มวันเกิดใหม่

- ข้อมูลการศึกษา: สุ่มชื่อสถานศึกษาใหม่
- ประสบการณ์การทำงาน: สุ่มชื่อบริษัทใหม่
- ภาพใบหน้า: นำเสนอภาพการ์ตูน หรือภาพที่อยู่ในคลังรูปภาพที่ไม่ใช่เจ้าของข้อมูลสารสนเทศ
- ข้อมูลชีวภาพ: สุ่มข้อมูลชีวภาพ
- รหัสบัญชีผู้ใช้งาน: สุ่มบัญชีผู้ใช้งานใหม่

3. การเข้ารหัสข้อมูล:

- ชื่อ: เข้ารหัสชื่อด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- เลขประจำตัวประชาชน: เข้ารหัสเลขประจำตัวประชาชนด้วยอัลกอริทึมการเข้ารหัส
- เบอร์โทรศัพท์: เข้ารหัสเบอร์โทรศัพท์ด้วยอัลกอริทึมการเข้ารหัส
- ที่อยู่ผู้มีเมล: เข้ารหัสที่อยู่ผู้มีเมลด้วยอัลกอริทึมการเข้ารหัส
- ที่อยู่: เข้ารหัสรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- วันเกิด: เข้ารหัสวันเกิดด้วยอัลกอริทึมการเข้ารหัส
- ข้อมูลการศึกษา: เข้ารหัสชื่อสถานศึกษาด้วยอัลกอริทึมการเข้ารหัส
- ประสบการณ์การทำงาน: เข้ารหัสชื่อบริษัทด้วยอัลกอริทึมการเข้ารหัส
- ภาพใบหน้า: เข้ารหัสข้อมูลภาพใบหน้าด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- ข้อมูลชีวภาพ: เข้ารหัสข้อมูลชีวภาพด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- รหัสบัญชีผู้ใช้งาน: เข้ารหัสรหัสบัญชีผู้ใช้งานด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

4. การใช้เทคนิคอื่น ๆ:

- การใช้ Pseudonymization: แทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลเทียม เช่น แทนชื่อ "สมชาย" ด้วย "A001"
- การใช้ Generalization: เปลี่ยนข้อมูลให้เป็นข้อมูลทั่วไป เช่น แทนที่ "กรุงเทพมหานคร" ด้วย "ภาคกลาง"

ข้อควรระวัง:

- Data Masking ไม่ได้ลบข้อมูลส่วนบุคคลออกถาวร ข้อมูลที่ถูกปกปิดอาจถูกกู้คืนได้โดยผู้เชี่ยวชาญ
- Data Masking ควรดำเนินการโดยคำนึงถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
- ควรมีมาตรการป้องกันข้อมูลที่เพียงพอ เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึงข้อมูล

Shareholder and Investor Personal Data Masking วิธีการและตัวอย่างของ Shareholder and Investor Personal Data

Masking

1. การปกปิดข้อมูลบางส่วน:

- ชื่อ: ปิดบังชื่อนามสกุล เหลือเพียงชื่อย่อ เช่น นาย ค. หรือ นางสาว ค.
- เลขประจำตัวประชาชน: ปิดบังตัวเลขบางส่วน เช่น 12-3XXX-XXXX-23-4
- เบอร์โทรศัพท์: ปิดบังตัวเลขบางส่วน เช่น 081-XXXX-XXXX
- ที่อยู่ผู้มีเมล: เปลี่ยนโดเมนอีเมล เช่น [อีเมลถูกนำออกแล้ว] เป็น [อีเมลถูกนำออกแล้ว]
- ที่อยู่: ปิดบังรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- ส่วนการถือหุ้น: ปิดบังจำนวนหุ้นที่ถือครอง เหลือเพียงเปอร์เซ็นต์การถือหุ้น
- หมายเลขรหัสสมาชิก: จากตัวอย่าง 1234-5678-9012 เป็น XXXX-XXXX-9012 แสดงตัวเลข 4 หลักสุดท้าย

- **หมายเลขทะเบียนรถ:** จากตัวอย่าง ABC-1234 เป็น XXX-1234 ปิดบังตัวอักษรแต่ยังคงแสดงตัวเลข 4 หลักสุดท้าย
- **ภาพใบหน้า:** ทำการเบลอภาพใบหน้าหรือใช้เทคนิคในการครอบคลุมส่วนของใบหน้า เช่น การใช้ Pixelation หรือ Gaussian Blur ปิดบังใบหน้าเพื่อให้ไม่สามารถระบุตัวตนได้ แต่ยังสามารถมองเห็นภาพรวมของบุคคล
- **ข้อมูลชีวภาพ:** เช่น ลายนิ้วมือ หรือการจดจำใบหน้า ควรถูกเข้ารหัส (Encryption) หรือถูกทำให้เป็นนิรนาม (Anonymization)
- **รหัสบัญชีผู้ใช้งาน:** จากตัวอย่าง user1234 เป็น uXXX1234 หรือ UXXXXXX แสดงเฉพาะตัวอักษรหรือตัวเลขบางส่วน ส่วนที่เหลือจะถูกปิดบังด้วย X หรือ *

2. การสุ่มข้อมูล:

- **ชื่อ:** สุ่มชื่อใหม่จากฐานข้อมูลทั่วไป
- **เลขประจำตัวประชาชน:** สุ่มเลขประจำตัวประชาชนใหม่ แต่ต้องไม่ซ้ำกับเลขประจำตัวประชาชนจริง
- **เบอร์โทรศัพท์:** สุ่มเบอร์โทรศัพท์ใหม่ แต่ต้องไม่ซ้ำกับเบอร์โทรศัพท์จริง
- **ที่อยู่ผู้มีเมล:** สุ่มโดเมนอีเมลใหม่
- **ที่อยู่:** สุ่มรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- **สัดส่วนการถือหุ้น:** สุ่มจำนวนหุ้นที่ถือครองใหม่
- **หมายเลขรหัสสมาชิก:** สุ่มรหัสสมาชิกใหม่
- **หมายเลขทะเบียนรถ:** สุ่มทะเบียนรถใหม่
- **ภาพใบหน้า:** นำเสนอภาพการ์ตูน หรือภาพที่อยู่ในคลังรูปภาพที่ไม่ใช่เจ้าของข้อมูลสารสนเทศ
- **ข้อมูลชีวภาพ:** สุ่มข้อมูลชีวภาพ
- **รหัสบัญชีผู้ใช้งาน:** สุ่มบัญชีผู้ใช้งานใหม่

3. การเข้ารหัสข้อมูล:

- **ชื่อ:** เข้ารหัสชื่อด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **เลขประจำตัวประชาชน:** เข้ารหัสเลขประจำตัวประชาชนด้วยอัลกอริทึมการเข้ารหัส
- **เบอร์โทรศัพท์:** เข้ารหัสเบอร์โทรศัพท์ด้วยอัลกอริทึมการเข้ารหัส
- **ที่อยู่ผู้มีเมล:** เข้ารหัสที่อยู่ผู้มีเมลด้วยอัลกอริทึมการเข้ารหัส
- **ที่อยู่:** เข้ารหัสรายละเอียดบางส่วน เช่น บ้านเลขที่ ถนน
- **สัดส่วนการถือหุ้น:** เข้ารหัสจำนวนหุ้นที่ถือครองด้วยอัลกอริทึมการเข้ารหัส
- **หมายเลขรหัสสมาชิก:** เข้ารหัสหมายเลขสมาชิกด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **หมายเลขทะเบียนรถ:** เข้ารหัสหมายเลขทะเบียนรถด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **ภาพใบหน้า:** เข้ารหัสข้อมูลภาพใบหน้าด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **ข้อมูลชีวภาพ:** เข้ารหัสข้อมูลชีวภาพด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256
- **รหัสบัญชีผู้ใช้งาน:** เข้ารหัสรหัสบัญชีผู้ใช้งานด้วยอัลกอริทึมการเข้ารหัส เช่น SHA-256

4. การใช้เทคนิคอื่นๆ:

- **การใช้ Pseudonymization:** แทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลเทียม เช่น แทนชื่อ "สมชาย" ด้วย "A001"
- **การใช้ Generalization:** เปลี่ยนข้อมูลให้เป็นข้อมูลทั่วไป เช่น แทนที่ "กรุงเทพมหานคร" ด้วย "ภาคกลาง"

ข้อควรระวัง:

- Data Masking ไม่ได้ลบข้อมูลส่วนบุคคลออกถาวร ข้อมูลที่ถูกปกปิดอาจถูกกู้คืนได้โดยผู้เชี่ยวชาญ
- Data Masking ควรดำเนินการโดยคำนึงถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
- ควรมีมาตรการป้องกันข้อมูลที่เพียงพอ เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึงข้อมูล

แนวทางปฏิบัตินี้ประกาศและมีผลตั้งแต่วันที่ 10 กันยายน 2568 เป็นต้นไป



พิจารณาอนุมัติ



ผู้อนุมัติ

(นายชนกร ชาลี)

ประธานเจ้าหน้าที่ฝ่ายปฏิบัติการ

วันที่ 10 กันยายน 2568