



บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)

แนวปฏิบัติการเปิดเผยข้อมูลส่วนบุคคลที่สำคัญ




Masking Data Privacy

รหัสเอกสาร :	GL-PDO-008
หมายเลขปรับปรุงเอกสาร :	2.0
วันที่เอกสารมีผลบังคับใช้ :	25 เมษายน 2566
เจ้าของเอกสาร :	PDPA Office
ผู้อนุมัติเอกสาร :	สุรัชย์ ชมเพลินใจ

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	คำอธิบายและเหตุผลในการแก้ไข	ผู้แก้ไข	วันที่
1.0	เอกสารเผยแพร่ ฉบับแรก	PDPA Office	1 กันยายน 2565
2.0	เพิ่มวิธีการทำ Eye View	PDPA Office	25 เมษายน 2566

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ	ลายเซ็น	ตำแหน่ง	วันที่
จัดทำโดย	รัชฎา ปิ่นสอยชัย		Administrator	25 เมษายน 2566
ตรวจทาน	วงศ์เดือน แซ่เตียว		Supervisor	25 เมษายน 2566
อนุมัติโดย	สุรัชย์ ชมเพลินใจ		เจ้าหน้าที่คุ้มครอง ข้อมูลส่วนบุคคล (DPO)	25 เมษายน 2566

เอกสารอ้างอิง

1. พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. PC-CS-001 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

## สารบัญ

	หน้า
1. วัตถุประสงค์	4
2. กำหนดข้อมูลส่วนบุคคลที่สำคัญ 18 รายการ ที่ต้องเฝ้าระวัง และมีการดูแลรักษาข้อมูลเป็นกรณีพิเศษ	4
3. กำหนดรูปแบบการเปิดเผย หรือการทำ Masking Data Privacy	5
4. หลักการและขั้นตอนการทำ Masking ของ 3BB (3BB Masking Solution)	7

## 1. วัตถุประสงค์

การกำหนดรูปแบบการเปิดเผยข้อมูลส่วนบุคคลที่สำคัญของลูกค้า พนักงาน หรืออื่น ๆ สำหรับรองรับ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ผู้ปฏิบัติงาน หรือ ผู้มีหน้าที่เกี่ยวข้องกับการเปิดเผยข้อมูลในรายงาน หน้าจอคอมพิวเตอร์ หน้าจอโทรศัพท์มือถือ หรือในอุปกรณ์พกพาอื่น ๆ ให้มีการแสดงข้อมูลส่วนบุคคลที่สำคัญ หรือการเปิดเผยข้อมูลเป็นไปตามมาตรฐานรักษาความปลอดภัยที่กำหนดขึ้น

Data Masking ถือเป็น Data Protection อย่างหนึ่ง เป็นการปกป้องข้อมูลที่สำคัญเมื่อมีการนำข้อมูลนั้นออกมาแสดงผล โดยทำการปกปิดหรือปิดบังข้อมูลเหล่านั้น เพื่อให้เป็นข้อมูลที่ไม่ตรงกับข้อมูลต้นฉบับที่แท้จริง ซึ่งทำให้ผู้ไม่ประสงค์ดีหรือผู้ที่ไม่มีความเกี่ยวข้องกับข้อมูลต้นฉบับเหล่านั้น ไม่สามารถนำไปใช้งานหรือทำธุรกรรมต่าง ๆ ได้

## 2. กำหนดข้อมูลส่วนบุคคลที่สำคัญ 18 รายการ ที่ต้องเฝ้าระวังและมีการดูแลรักษาข้อมูลเป็นกรณีพิเศษ

โดยข้อมูลที่สำคัญของบริษัท 3BB นั้น ได้กำหนดไว้ใน 18 Customer Data Privacy เรียบร้อยแล้ว ดังต่อไปนี้

ข้อมูลเดียวที่จัดว่าเป็น Customer Data Privacy

- 1) หมายเลขโทรศัพท์
- 2) หมายเลขบัญชีลูกค้า (Account Number)
- 3) ข้อมูลทางชีวภาพเช่นลายนิ้วมือ ม่านตา หรือ วัตถุที่ระบุตัวตน (Biometric Data)
- 4) หมายเลขบัตรเครดิตหรือเดบิต Credit/ Debit Card Number
- 5) ข้อมูลใดๆเกี่ยวกับราชวงศ์ (Royal Category)
- 6) หมายเลขบัตรประชาชนหรือหนังสือเดินทาง (Citizen ID/ Passport Number)
- 7) หมายเลขบัญชีธนาคาร (Bank Account Number)
- 8) สถานะแบล็คลิสต์ ของผู้ใช้บริการ (Blacklist Flag of customer)
- 9) ชื่อ – นามสกุล (Name – Surname)
- 10) อีเมลลูกค้า (Email address)

และข้อมูลดังต่อไปนี้ เมื่อรวมกับ 1) หมายเลขโทรศัพท์ หรือ 2) หมายเลขบัญชีลูกค้า (Account Number) ก็จะถูกจัดว่าเป็น Data Privacy เช่นกัน

- 11) ลายเซ็น (Signature)
- 12) ตำแหน่งพิกัดที่ติดตั้งของลูกค้า (Customer Installation)
- 13) การเข้าถึง Content ของผู้ใช้งาน (Content Accessed)
- 14) วันเกิด (Birthdate )
- 15) รูปถ่าย (Photo)



- 16) ข้อมูลติดต่อลูกค้าในการจัดส่งเอกสาร (Contact Information)
- 17) URL การใช้งาน Internet และ Application (URL Accessed/ Application)
- 18) ไฟล์บันทึกเสียง เช่น การบันทึกโทรเข้า Call Center (Voice record)

### 3. กำหนดรูปแบบการเปิดเผย หรือการทำ Masking Data Privacy

- 1) หมายเลขโทรศัพท์ แสดง 3 หลักท้าย เช่น XXXXXX789 (ตามรูปแบบ Encryption ระบบ BCS) หรือแสดง 3 หลักแรก และ 4 หลักสุดท้าย เช่น 081XXX6789
- 2) หมายเลขบัญชีลูกค้า (Account Number) แสดง 2 หลักแรก และ 4 หลักสุดท้าย เช่น 60XXX9333
- 3) ข้อมูลทางชีวภาพ เช่น ลายนิ้วมือ ม่านตา หรือ วัตถุที่ระบุตัวตน (Biometric Data) ไม่ต้องทำ masking เนื่องจากในตอนนี้ระบบยังไม่รองรับกับ masking ข้อมูลที่ไม่ใช่ตัวเลขหรือตัวอักษร
- 4) หมายเลขบัตรเครดิตหรือเดบิต (Credit/Debit Card Number) แสดง 6 หลักแรก และ 4 หลักสุดท้าย เช่น 123456XXXXXX1111 ซึ่งเป็นไปตามมาตรฐาน PCI DSS
- 5) หมายเลขบัตรประชาชนหรือหนังสือเดินทาง (Citizen ID / Passport Number) ใช้หลักการเดียวกันคือ แสดง 4 หลักสุดท้าย เช่น XXXXXX1234
- 6) หมายเลขบัญชีธนาคาร (Bank Account Number) แสดง 4 หลักแรก และ 3 หลักสุดท้าย เช่น 1234XXXXXX567
- 7) อีเมลล์ลูกค้า (Email address) แสดง 4 หลักแรก และหลังจากนั้นจะ mask ทั้งหมด เช่น ABCDx@xxx.xxx.xx (ABCDE@3bb.co.th)
- 8) ชื่อ-นามสกุล (Name-Surname) แสดงชื่อเต็ม และ mask นามสกุลด้วย XXXXX (X จำนวน 5 ตัว) เพื่อป้องกันการคาดเดานามสกุลที่เป็นไปได้ เมื่อทราบชื่อแล้ว และการ mask อีกรูปแบบหนึ่ง คือ แสดงแต่ 3 ตัวหน้า ทั้งชื่อและนามสกุล (X จำนวน 5 ตัว) (ตัวอย่าง สมทXXXXX รักXXXXX)
- 9) สถานะแบล็คลิสต์ของผู้ใช้บริการ (Blacklist flag of Customer) เปลี่ยน display name เป็น watch list
- 10) ข้อมูลใด ๆ เกี่ยวกับราชวงศ์ Royal Category ไม่มีการทำ masking แต่ผู้มี Authorize เท่านั้นที่เห็นข้อมูลเหล่านี้ สำหรับผู้ไม่มี Authorize ก็จะไม่เห็นข้อมูลในส่วนนี้

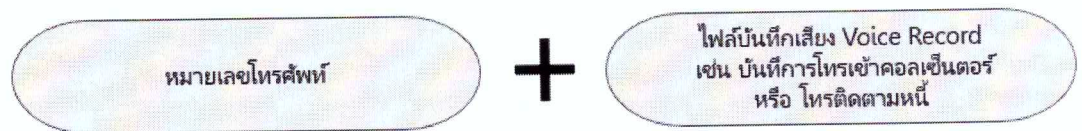
หมายเหตุ: สำหรับ fields ที่ 11 ถึง 18 ต้องอยู่ร่วมกับ 1) หมายเลขโทรศัพท์ หรือ 2) หมายเลขบัญชีลูกค้า (Account Number) ถึงจะเป็น sensitive fields แต่ถ้า field ที่ 1, 2 ได้ทำการ mask แล้ว fields ที่ 11-18 ก็ไม่ต้อง mask สามารถแสดงเป็น clear text ได้เลย

ข้อมูลหมายเลขบัญชีลูกค้า เบอร์โทรศัพท์ หรือ Username ที่มีการรวมกับข้อมูลอื่นถูกจัดว่าเป็น Customer Data Privacy ได้แก่

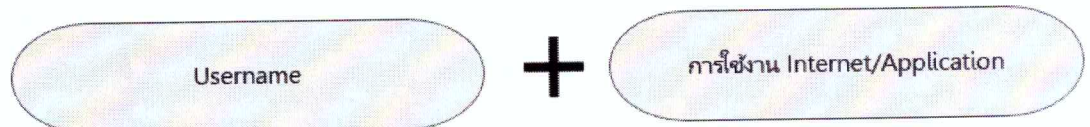
- ข้อมูลหมายเลขบัญชีลูกค้า รวมกับ



- หมายเลขโทรศัพท์ รวมกับ



- Username รวมกับ



#### 4. หลักการและขั้นตอนการทำ Masking ของ 3BB (3BB Masking Solution)

1. ทุกๆ applications จะต้องทำการ mask field ที่ 1-10 ทั้งหมดหากปรากฏอยู่บนหน้าจอของผู้ใช้งาน
2. หากผู้ใช้งานมีความจำเป็นต้องทราบข้อมูลต้นฉบับ เพื่อที่จะใช้งาน ก็สามารถกดปุ่ม Eye View ได้ โดยการกดปุ่ม Eye View นั้นจะเป็นการแสดงข้อมูลต้นฉบับ (Clear Text) โดยจะสามารถแบ่งเป็นทางเลือกได้ดังต่อไปนี้
  - 2.1. แสดงข้อมูลต้นฉบับทีละ field และเมื่อต้องการดู field ถัดไป ก็ให้กด Eye view ของ field นั้น โดยที่ field ก่อนหน้านั้นจะกลับมาถูก mask เหมือนตอนแรกที่เข้ามา
  - 2.2. แสดงข้อมูล sensitive fields ทั้งหมดที่มีอยู่ในหน้าจอหรือ screen โดยที่มีการกำหนดระยะเวลาของการแสดงเช่น 1 นาที (แล้วแต่ user จะเห็นเหมาะสม) เมื่อครบเวลาที่กำหนดแล้ว ทุกๆ field ก็ จะกลับมาถูก mask เหมือนตอนแรกที่เข้ามา
3. จะมีการบันทึก log จากการกดปุ่ม Eye View ทุกครั้ง ซึ่งจะสามารถระบุ user, applications, และวัน เวลาที่ user ใช้งานได้ โดยจะมีการเตรียม log center เพื่อรวบรวม log จากทุก application โดยหลักการของการเก็บ log นั้น local log จะต้องมีการจัดเก็บไม่ต่ำกว่า 90 วัน และ Archive Log ที่เราจะเก็บที่ central log นั้น จะเก็บไม่ต่ำกว่า 2 ปี ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
4. หากมี user ที่ไม่สามารถทำงานได้เลย จากการทำ data masking ดังที่กล่าวไว้ตามข้อ 1, 2, 3 ให้ปรึกษากับ DPO เป็นรายกรณีไป โดยจะต้องระบุถึงเหตุผลว่า ทำไมไม่สามารถทำการ masking ข้อมูลตามที่กำหนดได้ และจะมีวิธีการทำ Data Protection อย่างไรมาทดแทน ที่จะปกป้องข้อมูลส่วนบุคคลของลูกค้าได้อย่างปลอดภัย โดยแจ้งเรื่องมาที่ PDPA Office (E-Mail dpo@jasmine.com)

หมายเหตุ : พนักงานของบริษัททุกท่านที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลของลูกค้า ขอให้กำหนดสิทธิการเข้าถึงเท่าที่จำเป็นต่องานที่ต้องปฏิบัติ หรือได้รับมอบหมายเท่านั้น

อ้างอิงจากเอกสาร นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (PC-CS-001) ในหัวข้อ 2 กลยุทธ์การป้องกันความปลอดภัยของข้อมูล (Information Security Protection Strategy)

- (1) การขอสิทธิใหม่และการเพิ่มเติมสิทธิการเข้าถึงระบบคอมพิวเตอร์และบริการ ต้องได้รับอนุญาตตามหน้าที่ความรับผิดชอบและเท่าที่จำเป็นต่อการปฏิบัติงาน (Least Privilege)

หากท่านใดละเมิด กำหนดและใช้สิทธิเกินความจำเป็น จะถือว่าท่านทำผิดนโยบายของบริษัท ซึ่งในกรณีที่เกิดการตรวจสอบของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเข้ามาตรวจสอบในกรณีที่มีการร้องเรียนหรือพบว่าข้อมูลของลูกค้าถูกเปิดเผยออกไปโดยไม่ได้รับอนุญาต ท่านจะต้องได้รับโทษทางปกครอง ตามที่ระบุไว้ในพระราชบัญญัติคุ้มครองส่วนบุคคล พ.ศ. 2562