(ร่าง) แนวปฏิบัติธนาคารแห่งประเทศไทย
เรื่อง การรักษาความมั่นคงปลอดภัยของการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ประเภทการรู้จำใบหน้า (Facial Recognition) เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ

14 กันยายน 2569

ร่าง

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน

ธนาคารแห่งประเทศไทย

โทรศัพท์ 02-356-7019, 02-356-7827

e-mail: TSD-TechPolicy@bot.or.th

สารบัญ

1. เหตุผลในการออกแนวปฏิบัติ 3

2. แนวปฏิบัติที่ยกเลิก 3

3. ขอบเขตการใช้แนวปฏิบัติ 4

4. เนื้อหา 4

4.1 นิยาม 4

4.2 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ประเภทการรู้จำใบหน้า (Facial Recognition) เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ 7

ส่วนที่ 1 การรักษาความมั่นคงปลอดภัยของระบบ 8

ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติ 9

ส่วนที่ 3 การรักษาประสิทธิภาพของเทคโนโลยี 13

5. การแจ้ง การรายงาน หรือการขออนุญาต ต่อ ธปท. 14

5.1 การทดสอบ ตรวจประเมิน และรายงานผลภายหลังออกแนวปฏิบัติ 14

5.2 การแจ้งหรือการขออนุญาตนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีอย่างมีนัยสำคัญ 15

5.3 การหารือกรณีนำเทคโนโลยีชีวมิติประเภทอื่นมาใช้ หรือใช้เทคโนโลยี Facial Recognition เพื่อวัตถุประสงค์อื่น 17

ภาคผนวก ก กรอบการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า (Face Comparison) 18

ภาคผนวก ข กรอบการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection 21

แนวปฏิบัติธนาคารแห่งประเทศไทย
เรื่อง การรักษาความมั่นคงปลอดภัยของการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ประเภทการรู้จำใบหน้า (Facial Recognition) เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ

---

1. เหตุผลในการออกแนวปฏิบัติ

ปัจจุบัน ผู้ให้บริการนำเทคโนโลยีการรู้จำใบหน้า (Facial Recognition) มาใช้ในการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่อย่างแพร่หลาย ทั้งในการเปิดบัญชี การโอนเงิน การสมัครใช้บริการ และการทำธุรกรรมสำคัญอื่น ๆ โดยเทคโนโลยีดังกล่าวช่วยเพิ่มความน่าเชื่อถือของการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ และยกระดับความมั่นคงปลอดภัยในการให้บริการทางการเงินผ่านช่องทางดิจิทัล

อย่างไรก็ตาม ภัยคุกคามที่มุ่งโจมตีเทคโนโลยี Facial Recognition เกิดขึ้นอย่างต่อเนื่องและมีความซับซ้อนมากขึ้น โดยเฉพาะการใช้ปัญญาประดิษฐ์สร้างสื่อปลอม (AI Deepfake) เพื่อใช้ในการโจมตีด้วยการปลอมแปลงชีวมิติ (Presentation Attack) ซึ่งเพิ่มความเสี่ยงการสวมรอยผู้ใช้บริการเพื่อทำธุรกรรมโดยไม่ได้รับอนุญาต ดังนั้นหากผู้ให้บริการไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของเทคโนโลยี Facial Recognition อย่างเพียงพอ อาจก่อให้เกิดการทุจริตและความเสียหายต่อผู้ใช้บริการ รวมถึงส่งผลกระทบต่อความเชื่อมั่นของประชาชนต่อการใช้บริการทางการเงินผ่านช่องทางดิจิทัล

ธนาคารแห่งประเทศไทย (ธปท.) ตระหนักถึงความสำคัญของการป้องกันภัยคุกคามดังกล่าว จึงได้ออกแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ประเภทการรู้จำใบหน้า (Facial Recognition) เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ เพื่อยกระดับมาตรฐานการใช้เทคโนโลยีดังกล่าวให้มีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างเหมาะสม

2. แนวปฏิบัติที่ยกเลิก

แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน ตามหนังสือเวียนธนาคารแห่งประเทศไทยที่ ธปท.ฝนช.(09) ว. 689/2566 ลงวันที่ 29 กันยายน 2566

3. ขอบเขตการใช้แนวปฏิบัติ

แนวปฏิบัติฉบับนี้ใช้กับผู้ให้บริการที่อยู่ภายใต้การกำกับดูแลของ ธปท. และมีการใช้เทคโนโลยี Facial Recognition เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ดังต่อไปนี้

3.1 สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

3.2 สถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

3.3 ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน

3.4 ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อส่วนบุคคลภายใต้การกำกับ)

3.5 ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ)

4. เนื้อหา

4.1 นิยาม

ในแนวปฏิบัติฉบับนี้

“ผู้ให้บริการ” หมายความว่า สถาบันการเงินและสถาบันการเงินเฉพาะกิจตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลและผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 ที่มีการใช้เทคโนโลยี Facial Recognition เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่

“ผู้ใช้บริการ” หมายความว่า บุคคลธรรมดาหรือนิติบุคคลที่ใช้บริการของผู้ให้บริการ

“ผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน” หมายความว่า บุคคลภายนอกที่ผู้ให้บริการว่าจ้างหรือใช้บริการให้เป็นผู้ดำเนินการหรือรับผิดชอบกระบวนการพิสูจน์หรือยืนยันตัวตนของ

ผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition เช่น Identity Provider (IdP) หรือ Electronic Know Your Customer (eKYC) Provider

“เทคโนโลยีการรู้จำใบหน้า (Facial Recognition)” หรือ **“เทคโนโลยี Facial Recognition”** หมายความว่า เทคโนโลยีชีวมิติที่ใช้ลักษณะเฉพาะของใบหน้าในการเปรียบเทียบข้อมูลใบหน้า ซึ่งผู้ให้บริการนำมาใช้เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ

“ระบบ Facial Recognition” หมายความว่า ซอฟต์แวร์ ฮาร์ดแวร์ และองค์ประกอบอื่นที่เกี่ยวข้องกับการทำงานของเทคโนโลยี Facial Recognition และการเก็บรักษาข้อมูลใบหน้าของผู้ใช้บริการ

“การเปรียบเทียบภาพใบหน้า (Face Comparison)” หมายความว่า การนำข้อมูลใบหน้าจำนวนสองชุดมาเปรียบเทียบกัน เพื่อประเมินว่าข้อมูลใบหน้าทั้งสองข้อมูลเป็นของบุคคลเดียวกันหรือไม่

“การตรวจจับการปลอมแปลงชีวมิติ (Presentation Attack Detection: PAD)” หมายความว่า การตรวจสอบลักษณะทางชีวมิติที่นำเสนอต่อเทคโนโลยี Facial Recognition เพื่อแยกแยะว่าเป็นการนำเสนอลักษณะทางชีวมิติโดยตรงของบุคคลที่กำลังแสดงตน ณ จุดเก็บข้อมูล หรือเป็นการนำเสนอสื่อโจมตี

“ระบบ Presentation Attack Detection” หมายความว่า ซอฟต์แวร์ ฮาร์ดแวร์ และองค์ประกอบอื่นที่เกี่ยวข้องกับการทำงานของเทคโนโลยี Presentation Attack Detection

“การโจมตีด้วยการปลอมแปลงชีวมิติ (Presentation Attack)” หมายความว่า การนำเสนอสื่อโจมตีต่อเทคโนโลยี Facial Recognition โดยมีเจตนาหลอกเทคโนโลยีว่าเป็นการนำเสนอลักษณะทางชีวมิติโดยตรงของบุคคลที่กำลังแสดงตน ณ จุดเก็บข้อมูล

“สื่อโจมตี (Presentation Attack Instrument: PAI)” หมายความว่า สื่อ อุปกรณ์ หรือสิ่งอื่นใดที่ใช้ในการนำเสนอลักษณะทางชีวมิติต่อเทคโนโลยี Facial Recognition แทนการนำเสนอลักษณะทางชีวมิติโดยตรงของบุคคลที่กำลังแสดงตน ณ จุดเก็บข้อมูล

“สื่อโจมตีระดับความซับซ้อนต่ำ” หมายความว่า สื่อโจมตีที่บุคคลทั่วไปสามารถจัดเตรียมได้ภายในเวลาไม่เกิน 1 วัน และอาศัยข้อมูลหรือสื่อของเป้าหมายที่สามารถเข้าถึงได้ง่าย เช่น รูปภาพหรือวิดีโอจากแหล่งข้อมูลสาธารณะทั่วไป

“สื่อโจมตีระดับความซับซ้อนปานกลาง” หมายความว่า สื่อโจมตีที่ต้องอาศัยความรู้หรือความชำนาญในการจัดเตรียม โดยใช้เวลาจัดเตรียมไม่เกิน 1 สัปดาห์ หรืออาศัยข้อมูลหรือสื่อของเป้าหมายที่เข้าถึงได้ยากในระดับปานกลาง เช่น รูปภาพหรือวิดีโอที่ไม่สามารถเข้าถึงได้จากแหล่งข้อมูลสาธารณะทั่วไป

“สื่อโจมตีระดับความซับซ้อนสูง” หมายความว่า สื่อโจมตีที่ต้องอาศัยผู้เชี่ยวชาญในการจัดเตรียม โดยใช้เวลาจัดเตรียมมากกว่า 1 สัปดาห์ และอาศัยข้อมูลหรือสื่อของเป้าหมายที่เข้าถึงได้ยาก เช่น รูปภาพหรือวิดีโอที่มีรายละเอียดของใบหน้าในระดับที่สามารถนำไปใช้สร้างหน้ากากหรือหุ่นจำลองที่มีความสมจริงสูง

“ธุรกรรมทดสอบ” หมายความว่า การดำเนินการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition ที่มีผลการตัดสินจากเทคโนโลยี โดยไม่นับรวมความพยายามในการพิสูจน์หรือยืนยันตัวตน (Attempt) ที่เทคโนโลยีไม่สามารถประมวลผลจนได้ผลการตัดสิน

“กลุ่มตัวอย่าง” หมายความว่า บุคคลที่ข้อมูลใบหน้าถูกนำมาใช้ในการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า หรือถูกนำมาจัดทำสื่อโจมตีในการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection

“ผู้ดำเนินการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection” หมายความว่า บุคคลที่นำเสนอสื่อโจมตีต่อเทคโนโลยี Facial Recognition ในการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection

“False Match Rate (FMR)” หมายความว่า อัตราของการเปรียบเทียบภาพใบหน้าระหว่างบุคคลที่แตกต่างกันที่เทคโนโลยีตัดสินว่าเป็นบุคคลเดียวกัน

“Impostor Attack Presentation Accept Rate (IAPAR)” หมายความว่า อัตราที่เทคโนโลยี Presentation Attack Detection ไม่สามารถตรวจจับสื่อโจมตี จนเกิดการตัดสินว่าใบหน้าที่นำเสนอผ่านสื่อโจมตีเป็นบุคคลเดียวกันกับภาพใบหน้าอ้างอิง

“Liveness Detection” หมายความว่า การตรวจสอบและวิเคราะห์ว่าข้อมูลใบหน้าที่กำลังเก็บ (Capture) มาจากบุคคลที่มีชีวิตและกำลังแสดงตน ณ จุดเก็บข้อมูล

“Liveness Detection Setting” หมายความว่า ค่าหรือชุดการตั้งค่าที่กำหนดวิธีการหรือพารามิเตอร์ในการทำงานของเทคโนโลยี Liveness Detection เช่น การเลือกใช้ Passive

Liveness Detection การเลือกใช้ Active Liveness Detection หรือการกำหนด Challenge-Response Actions ที่ให้ผู้ใช้บริการปฏิบัติตาม

“ค่าเกณฑ์การตัดสินผล (Threshold)” หมายความว่า ค่าที่กำหนดเพื่อใช้เป็นเกณฑ์สำหรับการตัดสินผลของแต่ละขั้นตอนการทำงานของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection เช่น ค่าเกณฑ์สำหรับการประเมินคุณภาพของภาพใบหน้า (Face Image Quality Threshold) ค่าเกณฑ์สำหรับการตัดสินผลการเปรียบเทียบภาพใบหน้า (Face Comparison Threshold) ค่าเกณฑ์สำหรับการตัดสินผล Liveness Detection (Liveness Detection Threshold)

“ข้อมูลชีวมิติ (Biometric Data)” หมายความว่า ข้อมูลที่เกี่ยวข้องกับลักษณะทางชีวภาพของผู้ใช้บริการ ซึ่งรวมถึงข้อมูลใบหน้าและข้อมูลอ้างอิงชีวมิติ

“ข้อมูลอ้างอิงชีวมิติ (Biometric Reference)” หมายความว่า ข้อมูลชีวมิติที่ถูกใช้เป็นข้อมูลอ้างอิงในการเปรียบเทียบภาพใบหน้า

“Video Injection Attack” หมายความว่า การโจมตีที่ผู้โจมตีแทรกหรือส่งข้อมูลใบหน้าที่ถูกสร้าง ดัดแปลง หรือบันทึกไว้ล่วงหน้าเข้าสู่กระบวนการประมวลผลของเทคโนโลยี Facial Recognition หรือเทคโนโลยี Presentation Attack Detection

“การเก็บข้อมูลใบหน้าจากผู้ใช้บริการ (Face Data Capture)” หมายความว่า การรับหรือบันทึกข้อมูลใบหน้าของผู้ใช้บริการจากกล้องของอุปกรณ์เคลื่อนที่

“ข้อมูลใบหน้า” หมายความว่า ข้อมูลที่แสดงถึงลักษณะของใบหน้าของผู้ใช้บริการ ซึ่งอยู่ในรูปแบบภาพนิ่ง ภาพเคลื่อนไหว หรือวิดีโอ

4.2 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ประเภทการรู้จำใบหน้า (Facial Recognition) เพื่อพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ

ผู้ให้บริการต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของระบบ Facial Recognition ระบบ Presentation Attack Detection และข้อมูลชีวมิติให้ครอบคลุมทุกขั้นตอนของการทำงานของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection ตั้งแต่การเก็บข้อมูลใบหน้าจากผู้ใช้บริการ (Face Data Capture) การประมวลผลข้อมูลชีวมิติ (Signal Processing) การเก็บรักษาข้อมูลชีวมิติ (Biometric Data Storage) การเปรียบเทียบภาพใบหน้า (Face

Comparison) และการตัดสินผลการเปรียบเทียบภาพใบหน้า (Decision) รวมทั้งดูแลรักษาให้เทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection มีประสิทธิภาพเหมาะสมกับระดับความเสี่ยง เพื่อให้การพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition มีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างเหมาะสม

ส่วนที่ 1 การรักษาความมั่นคงปลอดภัยของระบบ

ผลลัพธ์ที่คาดหวัง: ระบบ Facial Recognition และระบบ Presentation Attack Detection ได้รับการออกแบบ ติดตั้ง ดูแลรักษา และเฝ้าระวังด้านความมั่นคงปลอดภัยอย่างเหมาะสมตลอดวงจรการใช้งาน

(1) จัดวางระบบ Facial Recognition และระบบ Presentation Attack Detection ภายในขอบเขตเครือข่าย (Network Zone) ที่เหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบ ระดับความสำคัญของข้อมูลที่ถูกประมวลผลและเก็บรักษา และความจำเป็นในการเชื่อมต่อกับระบบอื่น

(2) มีกระบวนการบริหารจัดการ Security Patch ระบบ Facial Recognition และระบบ Presentation Attack Detection ที่ครอบคลุมการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง Security Patch การทดสอบ Security Patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง และการติดตั้ง Security Patch บนระบบที่ให้บริการจริง โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่

ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง Security Patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ต้องจัดให้มีการควบคุมอื่นทดแทน

นอกจากนี้ กรณีที่ไม่สามารถติดตั้ง Security Patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น ดำเนินการประเมินความเสี่ยง และกำหนดมาตรการควบคุมความเสี่ยงที่เพียงพอและเหมาะสม

(3) ประเมินช่องโหว่ระบบ Facial Recognition และระบบ Presentation Attack Detection (Vulnerability Assessment) อย่างน้อยทุก 3 เดือน และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนเทคโนโลยี ผู้ให้บริการเทคโนโลยี หรือผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน การอัปเดตอัลกอริทึมหรือโมเดล และการปรับค่า Threshold พร้อมทั้งรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

(4) ทดสอบเจาะระบบ Facial Recognition และระบบ Presentation Attack Detection (Penetration Test) อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยขอบเขตการทดสอบอย่างน้อยต้องครอบคลุม Presentation Attack, Video Injection Attack และการโจมตีผ่าน API พร้อมทั้งรายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

ทั้งนี้ การทดสอบเจาะระบบอาจดำเนินการโดยผู้เชี่ยวชาญจากภายในหรือภายนอกองค์กรก็ได้ อย่างไรก็ตาม ผู้ดำเนินการทดสอบเจาะระบบด้วย Presentation Attack ต้องมีความเป็นอิสระจากผู้ดำเนินการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection เพื่อให้มั่นใจว่าผลการทดสอบเจาะระบบดำเนินการโดยผู้ที่มีความเป็นอิสระ และสะท้อนความเสี่ยงจากการโจมตีที่อาจเกิดขึ้นจริงได้อย่างเหมาะสม

(5) จัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับข้อมูลชีวมิติและการทำงานของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection ให้เพียงพอต่อการสนับสนุนการตรวจสอบ การสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัย และการใช้เป็นหลักฐานทางกฎหมาย โดยอย่างน้อยต้องสามารถติดตามเหตุการณ์สำคัญ เช่น การเข้าถึง การสร้าง การแก้ไข และการลบข้อมูลชีวมิติ การลงทะเบียนข้อมูลชีวมิติ การพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition ทั้งที่สำเร็จและไม่สำเร็จ การเปลี่ยนแปลงสิทธิการเข้าถึง และการเปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี

นอกจากนี้ ต้องมีมาตรการป้องกันการแก้ไขหรือทำลาย Log โดยไม่ได้รับอนุญาต และเก็บรักษา Log ย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติ

ส่วนที่ 2.1 การเก็บข้อมูลใบหน้าจากผู้ใช้บริการ (Face Data Capture)

ผลลัพธ์ที่คาดหวัง: ข้อมูลชีวมิติมีคุณภาพ ถูกต้องเชื่อถือได้ และกระบวนการเก็บข้อมูลใบหน้าดำเนินการบนสภาพแวดล้อมที่ปลอดภัย

(1) จัดให้มีกลไกตรวจจับการใช้งานเทคโนโลยี Facial Recognition บนอุปกรณ์หรือสภาพแวดล้อมที่มีความเสี่ยงด้านความมั่นคงปลอดภัย โดยอย่างน้อยต้องสามารถตรวจจับการใช้งานบน Rooted/Jailbroken Device และอุปกรณ์หรือสภาพแวดล้อมที่จำลองการทำงานของอุปกรณ์จริง

เช่น Virtual Device, Emulator และ Simulator รวมทั้งทบทวนและปรับปรุงกลไกดังกล่าวอย่างสม่ำเสมอ เพื่อให้สามารถรับมือกับเทคนิคหรือเครื่องมือหลีกเลี่ยงการตรวจจับที่มีการพัฒนาอย่างต่อเนื่อง

ทั้งนี้ เมื่อตรวจพบการใช้งานเทคโนโลยี Facial Recognition บนอุปกรณ์หรือสภาพแวดล้อมที่มีความเสี่ยงดังกล่าว ต้องปฏิเสธการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition

(2) จัดให้มีกลไกป้องกันการวิเคราะห์โครงสร้างและการทำงานของแอปพลิเคชันที่ใช้เทคโนโลยี Facial Recognition (Reverse Engineering) โดยอย่างน้อยต้องทำให้โค้ดของแอปพลิเคชันอ่านหรือวิเคราะห์ได้ยาก (Code Obfuscation) รวมทั้งทบทวนและปรับปรุงกลไกดังกล่าวอย่างสม่ำเสมอ

(3) จัดให้มีกลไกตรวจจับการดัดแปลงหรือการแทรกแซงการทำงานของแอปพลิเคชันที่ใช้เทคโนโลยี Facial Recognition เช่น Anti-Tampering, Anti-Hooking, Anti-Debugging, Runtime Integrity Check และ SDK Integrity Check รวมทั้งทบทวนและปรับปรุงกลไกดังกล่าวอย่างสม่ำเสมอ

ทั้งนี้ เมื่อตรวจพบการดัดแปลงหรือการแทรกแซงการทำงานดังกล่าว ต้องปฏิเสธการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition

(4) ไม่เก็บรักษาข้อมูลใบหน้าที่เก็บมาจากผู้ใช้บริการในกระบวนการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition ไว้ในอุปกรณ์เคลื่อนที่ของผู้ใช้บริการหลังจากเสร็จสิ้นกระบวนการดังกล่าว

(5) จัดให้มีคำแนะนำแก่ผู้ใช้บริการเกี่ยวกับสภาพแวดล้อม วิธีการเก็บข้อมูลใบหน้าและการเคลื่อนไหวใบหน้าตามคำสั่งในระหว่างการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition เช่น การจัดให้มีแสงสว่างที่เพียงพอ การหลีกเลี่ยงสิ่งปกปิดใบหน้า การจัดตำแหน่งใบหน้าให้อยู่ภายในกรอบที่กำหนด และการหันหน้าตามคำสั่ง เพื่อให้ผู้ใช้บริการสามารถดำเนินการตามขั้นตอนได้อย่างถูกต้อง และระบบได้รับข้อมูลใบหน้าที่มีคุณภาพเพียงพอและเหมาะสมต่อการประมวลผลของเทคโนโลยี Facial Recognition

ในกรณีที่มีการกำหนดให้ผู้ใช้บริการถอดแว่นในระหว่างการเก็บข้อมูลใบหน้า ต้องจัดให้มีกลไกที่ช่วยให้ผู้ใช้บริการรับทราบและปฏิบัติตามคำสั่งได้อย่างถูกต้องจนจบกระบวนการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition เช่น การแสดงคำสั่งด้วยข้อความหรือสัญลักษณ์ที่สามารถมองเห็นได้อย่างชัดเจนโดยไม่ต้องสวมแว่น หรือการให้คำแนะนำด้วยเสียง

(6) กำหนดเกณฑ์คุณภาพของข้อมูลใบหน้าที่ผู้ใช้บริการเก็บผ่านกล้องของอุปกรณ์เคลื่อนที่ (Selfie) ให้มีคุณภาพเพียงพอและเหมาะสมต่อการประมวลผลของเทคโนโลยี Facial Recognition โดยเกณฑ์ดังกล่าวต้องครอบคลุมปัจจัยที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี เช่น ความละเอียดและความคมชัดของภาพ ลักษณะและขนาดของใบหน้า และการไม่มีใบหน้าอื่นในตำแหน่งที่อาจรบกวนการประมวลผล

นอกจากนี้ ต้องตรวจสอบคุณภาพของข้อมูลใบหน้าที่ผู้ใช้บริการ Selfie ก่อนบันทึกเข้าระบบหรือนำไปใช้ และเมื่อพบว่าข้อมูลใบหน้าไม่เป็นไปตามเกณฑ์คุณภาพที่กำหนด ต้องปฏิเสธการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition

(7) จัดให้มีเทคโนโลยี Presentation Attack Detection เพื่อช่วยตรวจจับ Presentation Attack และเมื่อตรวจพบต้องปฏิเสธการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition

ทั้งนี้ สำหรับธุรกรรมที่มีความเสี่ยงสูง อาจพิจารณาใช้เทคโนโลยี Liveness Detection แบบ Active ที่ผู้ใช้บริการต้องตอบสนองต่อ Challenge ที่ระบบสุ่มขึ้น (Randomized Active Liveness Detection) ระหว่างการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition เช่น การให้ผู้ใช้บริการเคลื่อนไหวใบหน้าตามคำสั่งที่ระบบสุ่มขึ้น หรือการฉายแสงหรือสีต่าง ๆ บนใบหน้าในลำดับแบบสุ่ม

(8) จัดให้มีกลไกป้องกันการนำ Request หรือข้อมูลที่ใช้ในการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition กลับมาใช้ซ้ำโดยไม่ได้รับอนุญาต (Replay Attack) รวมทั้งกำหนดระยะเวลาที่ Request หรือข้อมูลดังกล่าวสามารถใช้งานได้อย่างเหมาะสม เช่น การใช้กลไก Challenge-Response ร่วมกับค่า Nonce หรือค่าที่ใช้ได้เพียงครั้งเดียว (One-time Value)

ส่วนที่ 2.2 การประมวลผลและการเก็บรักษาข้อมูลชีวมิติ (Signal Processing and Biometric Data Storage)

ผลลัพธ์ที่คาดหวัง: ข้อมูลชีวมิติได้รับการควบคุมการเข้าถึง การรักษาความลับ ความถูกต้องครบถ้วน และความน่าเชื่อถืออย่างเหมาะสม

(1) เก็บรักษาข้อมูลใบหน้า ข้อมูลอ้างอิงชีวมิติ และข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการที่จำเป็นต่อการทำงานของเทคโนโลยี Facial Recognition แยกจากกัน โดยอย่างน้อยต้องมีการแยกข้อมูลแบบ Logical Separation เช่น การแยกฐานข้อมูลหรือตารางข้อมูล (Table) รวมทั้งกำหนดสิทธิการเข้าถึงข้อมูลดังกล่าวแยกจากกัน

นอกจากนี้ ต้องไม่ใช้ข้อมูลที่สามารถระบุตัวตนของผู้ใช้บริการได้โดยตรง เช่น ชื่อ เลขประจำตัวประชาชน หมายเลขหนังสือเดินทาง หรือหมายเลขลูกค้า เป็นชื่อไฟล์หรือรหัสที่ใช้เชื่อมโยงข้อมูลใบหน้าหรือข้อมูลอ้างอิงชีวมิติ โดยอาจใช้รหัสที่สร้างขึ้นเพื่อวัตถุประสงค์ดังกล่าวโดยเฉพาะ เช่น ค่าที่สร้างขึ้นแบบสุ่ม เพื่อจำกัดผลกระทบในกรณีที่ข้อมูลใบหน้าหรือข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการถูกเข้าถึงโดยไม่ได้รับอนุญาต

ในกรณีที่ผู้ให้บริการใช้บริการเทคโนโลยี Facial Recognition จากบุคคลภายนอก เช่น ผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน หรือผู้ให้บริการเทคโนโลยี Facial Recognition ในรูปแบบ Software as a Service ผู้ให้บริการต้องกำกับดูแลไม่ให้บุคคลภายนอกดังกล่าวเก็บรักษาข้อมูลใบหน้าของผู้ใช้บริการ เว้นแต่การเก็บรักษาดังกล่าวเป็นการปฏิบัติตามที่กฎหมายกำหนด

(2) จัดให้มีการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) สำหรับการเข้าถึงข้อมูลชีวมิติ และการกำหนดหรือเปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection เช่น ค่า Threshold รวมทั้งกำหนดสิทธิการเข้าถึงตามหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) พร้อมทั้งทบทวนความเหมาะสมของสิทธิการเข้าถึงอย่างสม่ำเสมอ และเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของผู้ใช้งาน

ในกรณีที่ระบบไม่รองรับการพิสูจน์ตัวตนแบบหลายปัจจัย ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น ดำเนินการประเมินความเสี่ยง และกำหนดมาตรการควบคุมความเสี่ยงที่เพียงพอและเหมาะสม

(3) เข้ารหัสและตรวจสอบความถูกต้องครบถ้วน (Integrity) ของข้อมูลชีวมิติที่เกี่ยวข้องกับเทคโนโลยี Facial Recognition ทั้งขณะจัดเก็บ (Data at Rest) และขณะรับส่งข้อมูล (Data in Transit) โดยใช้อัลกอริทึม ความยาวกุญแจเข้ารหัส รวมทั้งช่องทางและวิธีการสื่อสารที่มีความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับโดยทั่วไป

นอกจากนี้ ต้องมีการบริหารจัดการกุญแจเข้ารหัสที่เหมาะสมตลอดวงจรชีวิตของกุญแจเข้ารหัส ครอบคลุมการสร้าง การเก็บรักษา การแจกจ่าย การหมุนเวียน การเพิกถอน และการทำลายกุญแจเข้ารหัส

(4) จัดให้มีกระบวนการยกเลิกการใช้งานข้อมูลอ้างอิงชีวมิติเดิมและลงทะเบียนข้อมูลอ้างอิงชีวมิติใหม่ เมื่อพบหรือมีเหตุอันควรสงสัยว่าข้อมูลอ้างอิงชีวมิติถูกเปิดเผยหรือเข้าถึงโดยไม่ได้รับอนุญาต และเมื่อถึงระยะเวลาหรือเงื่อนไขที่กำหนด เช่น เมื่อผู้ใช้บริการเปลี่ยนบัตรประจำตัว

ประชาชน ทั้งนี้ ต้องยืนยันตัวตนผู้ใช้บริการด้วยวิธีที่มีความมั่นคงปลอดภัยก่อนดำเนินการลงทะเบียนข้อมูลอ้างอิงชีวมิติใหม่

ส่วนที่ 2.3 การเปรียบเทียบภาพใบหน้าและการตัดสินผลการเปรียบเทียบภาพใบหน้า (Face Comparison and Decision)

ผลลัพธ์ที่คาดหวัง: ระบบไม่เปิดเผยผลการเปรียบเทียบภาพใบหน้าแก่ระบบหรือบุคคลที่ไม่เกี่ยวข้อง และมีการป้องกันการพยายามพิสูจน์หรือยืนยันตัวตนที่ผิดปกติ

(1) จำกัดการเปิดเผยผลการเปรียบเทียบภาพใบหน้าของเทคโนโลยี Facial Recognition เช่น Comparison Score หรือ Similarity Score โดยเปิดเผยข้อมูลดังกล่าวเท่าที่จำเป็น และไม่เปิดเผยผ่านช่องทางที่ทำให้ผู้ใช้บริการหรือบุคคลที่ไม่เกี่ยวข้องสามารถทราบหรือเข้าถึงข้อมูลดังกล่าวได้

(2) จำกัดจำนวนครั้งที่ผู้ใช้บริการสามารถพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition แล้วไม่สำเร็จติดต่อกัน และจัดให้มีการตอบสนองที่เหมาะสมเมื่อจำนวนครั้งดังกล่าวถึงเกณฑ์ที่กำหนด โดยกำหนดจำนวนครั้งและการตอบสนองให้สอดคล้องกับมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับโดยทั่วไป เช่น อนุญาตให้ผู้ใช้บริการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition แล้วไม่สำเร็จติดต่อกันได้ไม่เกิน 10 ครั้ง เมื่อจำนวนครั้งที่ไม่สำเร็จติดต่อกันถึงเกณฑ์ดังกล่าว ระบบจะหน่วงเวลาอย่างน้อย 30 วินาทีก่อนอนุญาตให้ผู้ใช้บริการพิสูจน์หรือยืนยันตัวตนในครั้งถัดไป นอกจากนี้ กรณีที่จำนวนครั้งที่ไม่สำเร็จติดต่อกันครบ 100 ครั้ง ระบบจะระงับการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยเทคโนโลยี Facial Recognition พร้อมจัดให้มีวิธีการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการด้วยวิธีการอื่นที่มีระดับความมั่นคงปลอดภัยเหมาะสมทดแทน[1]

ส่วนที่ 3 การรักษาประสิทธิภาพของเทคโนโลยี

ผลลัพธ์ที่คาดหวัง: เทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection มีประสิทธิภาพสอดคล้องตามมาตรฐานสากล โดยมีความแม่นยำของการเปรียบเทียบภาพใบหน้าและความสามารถในการตรวจจับสื่อโจมตีได้ตามเกณฑ์ที่กำหนด รวมทั้งมีกระบวนการติดตามประเมิน และปรับปรุงประสิทธิภาพของเทคโนโลยีอย่างต่อเนื่อง

(1) กำหนดเกณฑ์ประสิทธิภาพของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection ให้สอดคล้องกับมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับ

[1] อ้างอิงแนวทางตาม NIST SP 800-63B

โดยทั่วไป โดยกำหนดให้ค่า FMR ไม่เกิน 0.01%[2] และค่า IAPAR สำหรับสื่อโจมตีแต่ละประเภทไม่เกิน 4%

(2) ทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและเทคโนโลยี Presentation Attack Detection ตามกรอบการทดสอบที่กำหนดในภาคผนวก ก และภาคผนวก ข ตามลำดับ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ทั้งนี้ การทดสอบดังกล่าวอาจดำเนินการโดยผู้ดำเนินการทดสอบจากภายในหรือภายนอกองค์กรก็ได้ แต่ผู้ดำเนินการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection ต้องมีความเป็นอิสระจากผู้ดำเนินการทดสอบเจาะระบบด้วย Presentation Attack

(3) จัดให้มีกระบวนการเฝ้าระวัง ตรวจสอบ และตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับประสิทธิภาพและความมั่นคงปลอดภัยของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection โดยครอบคลุมกรณีที่พบความผิดปกติหรือแนวโน้มประสิทธิภาพลดลง เช่น ค่า FMR หรือค่า IAPAR สำหรับสื่อโจมตีประเภทใดประเภทหนึ่งเพิ่มขึ้นจนเกินเกณฑ์ประสิทธิภาพที่กำหนด รวมทั้งกรณีที่ได้รับข้อมูลเกี่ยวกับภัยคุกคาม ช่องโหว่ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อประสิทธิภาพหรือความมั่นคงปลอดภัยของเทคโนโลยี

5. การแจ้ง การรายงาน หรือการขออนุญาต ต่อ ธปท.

5.1 การทดสอบ ตรวจประเมิน และรายงานผลภายหลังออกแนวปฏิบัติ

สำหรับผู้ให้บริการที่นำเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection มาใช้งานอยู่แล้ว ต้องจัดให้มีการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า การทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection และการตรวจประเมินการปฏิบัติตามแนวปฏิบัติฉบับนี้ พร้อมรายงานผลการทดสอบและผลการตรวจประเมินต่อ ธปท. ภายใน 90 วัน นับแต่วันถัดจากวันที่ออกแนวปฏิบัติฉบับนี้

ในกรณีที่ผู้ให้บริการมีผลการทดสอบหรือผลการตรวจประเมินการปฏิบัติตามแนวปฏิบัติฉบับเดิมที่ดำเนินการก่อนวันที่ ธปท. ออกแนวปฏิบัติฉบับนี้ ผู้ให้บริการอาจนำผลดังกล่าวมารายงานต่อ ธปท. ได้ หากเป็นไปตามเงื่อนไขดังต่อไปนี้

(1) ผลการทดสอบหรือผลการตรวจประเมินมีอายุไม่เกิน 1 ปีนับแต่วันที่ ธปท. ออกแนวปฏิบัติฉบับนี้

---

[2] อ้างอิงแนวทางการกำหนดค่า False Match Rate (FMR) ตาม NIST SP 800-63B

(2) ข้อกำหนดการทดสอบหรือประเด็นที่ตรวจประเมินสอดคล้องตามที่กำหนดในแนวปฏิบัติฉบับนี้

ทั้งนี้ หากข้อกำหนดการทดสอบหรือประเด็นที่ตรวจประเมินยังไม่ครบถ้วนตามที่กำหนดในแนวปฏิบัติฉบับนี้ ผู้ให้บริการต้องจัดให้มีการทดสอบหรือการตรวจประเมินเพิ่มเติมในส่วนที่ยังไม่ครบถ้วนก่อนรายงานต่อ ธปท.

สำหรับปีถัดไป ผู้ให้บริการต้องจัดให้มีการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection อย่างน้อยปีละ 1 ครั้ง ตามที่กำหนดในส่วนที่ 3 (2) ของแนวปฏิบัติฉบับนี้ โดยไม่ต้องรายงานผลการทดสอบต่อ ธปท. ทั้งนี้ ธปท. อาจกำหนดให้ผู้ให้บริการรายงานผลการทดสอบดังกล่าว หรือจัดให้มีการทดสอบเพิ่มเติมเป็นรายกรณี เช่น เมื่อพบการโจมตีรูปแบบใหม่ที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี

สำหรับผู้ให้บริการที่ยังจัดส่งรายงานการใช้เทคโนโลยีชีวมิติแก่ ธปท. ตามแบบรายงานเดิมอย่างต่อเนื่อง ให้ยุติการจัดส่งรายงานดังกล่าวตั้งแต่วันถัดจากวันที่ออกแนวปฏิบัติฉบับนี้

5.2 การแจ้งหรือการขออนุญาตนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีอย่างมีนัยสำคัญ

ในกรณีที่ผู้ให้บริการนำเทคโนโลยี Facial Recognition หรือเทคโนโลยี Presentation Attack Detection มาใช้ใหม่ หรือมีการเปลี่ยนเทคโนโลยี ผู้ให้บริการเทคโนโลยี หรือผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน ผู้ให้บริการต้องจัดให้มีการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า การทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection และการตรวจประเมินการปฏิบัติตามแนวปฏิบัติฉบับนี้

ทั้งนี้ ในกรณีที่เป็นการนำเทคโนโลยี Presentation Attack Detection มาใช้ใหม่ หรือมีการเปลี่ยนเทคโนโลยี ผู้ให้บริการเทคโนโลยี หรือผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน ซึ่งการนำมาใช้ใหม่หรือการเปลี่ยนดังกล่าวไม่มีผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้า ผู้ให้บริการสามารถยกเว้นการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าได้

ในกรณีที่ผู้ให้บริการมีการเปลี่ยนแปลงระบบหรือเทคโนโลยี Facial Recognition หรือ Presentation Attack Detection อย่างมีนัยสำคัญกรณีอื่น ผู้ให้บริการต้องจัดให้มีการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection

ทั้งนี้ ในกรณีที่เป็นการเปลี่ยนแปลงระบบหรือเทคโนโลยี Presentation Attack Detection อย่างมีนัยสำคัญกรณีอื่น ซึ่งการเปลี่ยนแปลงดังกล่าวไม่มีผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้า ผู้ให้บริการสามารถยกเว้นการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าได้

ตารางสรุปแนวทางการทดสอบและการตรวจประเมินเมื่อมีการนำเทคโนโลยีมาใช้ใหม่หรือมีการเปลี่ยนแปลงระบบหรือเทคโนโลยีอย่างมีนัยสำคัญ

กรณี	**การทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า**	**การทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection**	**การตรวจประเมินการปฏิบัติตามแนวปฏิบัติ**
นำเทคโนโลยี Facial Recognition มาใช้ใหม่ หรือมีการเปลี่ยนเทคโนโลยีผู้ให้บริการเทคโนโลยี หรือผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน	✓	✓	✓
นำเทคโนโลยี Presentation Attack Detection มาใช้ใหม่ หรือมีการเปลี่ยนเทคโนโลยีหรือผู้ให้บริการเทคโนโลยี	เฉพาะเมื่อมีผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้า	✓	✓
เปลี่ยนแปลงระบบหรือเทคโนโลยี Facial Recognition อย่างมีนัยสำคัญกรณีอื่น	✓	✓	-
เปลี่ยนแปลงระบบหรือเทคโนโลยี Presentation Attack Detection อย่างมีนัยสำคัญกรณีอื่น	เฉพาะเมื่อมีผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้า	✓	-

5.3 การหารือกรณีนำเทคโนโลยีชีวมิติประเภทอื่นมาใช้ หรือใช้เทคโนโลยี Facial Recognition เพื่อวัตถุประสงค์อื่น

ในกรณีที่ผู้ให้บริการต้องการนำเทคโนโลยีชีวมิติประเภทอื่นมาใช้กับผู้ใช้บริการ เช่น เทคโนโลยีการรู้จำม่านตา (Iris Recognition) หรือเทคโนโลยีการรู้จำลายนิ้วมือ (Fingerprint Recognition) หรือต้องการนำเทคโนโลยี Facial Recognition มาใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ ผู้ให้บริการต้องหารือกับ ธปท. ก่อนดำเนินการ

ภาคผนวก ก กรอบการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า (Face Comparison)

การเปรียบเทียบภาพใบหน้าเป็นกลไกสำคัญในการพิสูจน์หรือยืนยันตัวตนผู้ใช้บริการ หากเทคโนโลยีมีความแม่นยำไม่เพียงพอ อาจส่งผลให้เกิดการยอมรับบุคคลที่ไม่ใช่เจ้าของตัวตน หรือปฏิเสธผู้ใช้บริการที่เป็นเจ้าของตัวตนจริงได้ ดังนั้น ผู้ให้บริการจึงควรจัดให้มีการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าโดยใช้ข้อมูลทดสอบที่มีความหลากหลายและสะท้อนการใช้งานจริง เพื่อให้มั่นใจว่าเทคโนโลยีสามารถรักษาระดับประสิทธิภาพและรองรับการให้บริการได้อย่างเหมาะสมตลอดอายุการใช้งานของระบบ

การทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้าแต่ละชุด ต้องเป็นไปตามข้อกำหนดขั้นต่ำดังต่อไปนี้

1. การตั้งค่าของเทคโนโลยี Facial Recognition

1.1 ทดสอบโดยใช้การตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้า เช่น ค่า Face Comparison Threshold ให้สอดคล้องกับการใช้งานจริง

1.2 ไม่เปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าตลอดการทดสอบ

2. จำนวนธุรกรรมทดสอบ การเลือกกลุ่มตัวอย่าง และสื่อที่ใช้ในการทดสอบ

2.1 ทดสอบด้วยจำนวนธุรกรรมทดสอบอย่างน้อย 300,000 ธุรกรรม ในกรณีที่กำหนดค่า FMR เป้าหมายไม่เกิน 0.01% โดยคำนวณจำนวนธุรกรรมทดสอบขั้นต่ำจากสูตร $\frac{30}{\text{ค่า FMR เป้าหมาย}}$

2.2 ทดสอบด้วยจำนวนกลุ่มตัวอย่างอย่างน้อย 776 ราย ในกรณีที่กำหนดจำนวนธุรกรรมทดสอบอย่างน้อย 300,000 ธุรกรรม โดยคำนวณจำนวนกลุ่มตัวอย่างขั้นต่ำจากสูตร

$$\frac{1 + \sqrt{\left(1 + \left(8 \times \text{จำนวนธุรกรรมทดสอบ}\right)\right)}}{2}$$

2.3 เลือกกลุ่มตัวอย่างให้สอดคล้องกับกลุ่มผู้ใช้บริการจริงหรือกลุ่มผู้ใช้บริการเป้าหมาย เช่น กรณีที่ผู้ใช้บริการส่วนใหญ่เป็นคนไทย กลุ่มตัวอย่างควรประกอบด้วยคนไทยในสัดส่วนไม่น้อยกว่าร้อยละ 80 ของจำนวนกลุ่มตัวอย่างทั้งหมด เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีภายใต้

ลักษณะประชากรที่ใกล้เคียงกับผู้ใช้งานจริง และลดความคลาดเคลื่อนจากการใช้กลุ่มตัวอย่างที่ไม่สอดคล้องกับบริบทการใช้งาน

2.4 เลือกกลุ่มตัวอย่างให้มีการกระจายตัวของเพศอย่างเหมาะสม เช่น เพศชายและเพศหญิงมีสัดส่วนอยู่ระหว่างร้อยละ 40 ถึง 60 ของจำนวนกลุ่มตัวอย่างทั้งหมด[3] เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีในการเปรียบเทียบภาพใบหน้าของผู้ใช้บริการทั้งเพศชายและเพศหญิง

2.5 เลือกกลุ่มตัวอย่างให้มีการกระจายตัวของช่วงอายุอย่างเหมาะสม เช่น กลุ่มตัวอย่างครอบคลุมช่วงอายุ 18–30 ปี 31–50 ปี และ 51–70 ปี โดยแต่ละช่วงอายุมีสัดส่วนอยู่ระหว่างร้อยละ 25 ถึง 40 ของจำนวนกลุ่มตัวอย่างทั้งหมด[4] เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีในการเปรียบเทียบภาพใบหน้าของผู้ใช้บริการในหลากหลายช่วงอายุ

2.6 ภาพใบหน้าที่ใช้ในการทดสอบต้องเป็นไปตามเกณฑ์คุณภาพที่กำหนดไว้ เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีในการใช้งานจริง

2.7 ประเภทของภาพใบหน้าที่ใช้ในการทดสอบต้องสอดคล้องกับประเภทของภาพใบหน้าที่ใช้ในการใช้งานจริง เช่น กรณีที่การใช้งานจริงเป็นการเปรียบเทียบภาพ Selfie กับภาพจากชิปบนบัตรประจำตัวประชาชน ผู้ให้บริการต้องจัดให้มีการทดสอบด้วยการเปรียบเทียบภาพในรูปแบบเดียวกัน โดยไม่ใช้ภาพ Selfie ที่จัดเก็บไว้ก่อนหน้าแทนภาพจากชิปบนบัตรประจำตัวประชาชน เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีในการใช้งานจริง

3. ผลการทดสอบ

3.1 คำนวณค่า FMR จากสูตร:

$$\text{FMR} = \left(\frac{\text{จำนวนธุรกรรมทดสอบเปรียบเทียบภาพใบหน้าระหว่างบุคคลที่แตกต่างกันที่เทคโนโลยีตัดสินว่าเป็นบุคคลเดียวกัน}}{\text{จำนวนธุรกรรมทดสอบเปรียบเทียบภาพใบหน้าระหว่างบุคคลที่แตกต่างกันทั้งหมด}} \right) \times 100$$

[3] อ้างอิงสัดส่วนการกระจายตัวของเพศตาม ISO/IEC 19795-5

[4] อ้างอิงสัดส่วนการกระจายตัวของช่วงอายุตาม ISO/IEC 19795-5

<u>ตัวอย่างการคำนวณ</u> ทดสอบเปรียบเทียบภาพใบหน้าระหว่างบุคคลที่แตกต่างกันจำนวน 300,700 ธุรกรรมทดสอบ และพบว่าเทคโนโลยีตัดสินว่าเป็นบุคคลเดียวกันจำนวน 25 ธุรกรรมทดสอบ

ดังนั้น FMR = $\left(\frac{25}{300,700}\right)$ x 100 = 0.0083%

ในกรณีที่ผู้ให้บริการนำเทคโนโลยี Facial Recognition มาใช้กับหลายประเภทธุรกรรม เช่น การเปิดบัญชีและการโอนเงิน และมีการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้า เช่น ค่า Face Comparison Threshold แตกต่างกันในแต่ละประเภทธุรกรรม หรือใช้ประเภทของภาพใบหน้าอ้างอิง เช่น ภาพจากชิปบนบัตรประจำตัวประชาชน หรือภาพ Selfie ที่จัดเก็บไว้ก่อนหน้า แตกต่างกันในแต่ละประเภทธุรกรรม ผู้ให้บริการต้องจัดให้มีการทดสอบแยกตามแต่ละรูปแบบการตั้งค่าและประเภทของภาพใบหน้าอ้างอิง โดยในการทดสอบแต่ละชุด ต้องใช้การตั้งค่าเพียงหนึ่งรูปแบบ และใช้ภาพใบหน้าอ้างอิงเพียงหนึ่งประเภทตลอดการทดสอบ

<u>ตัวอย่าง</u> ผู้ให้บริการนำเทคโนโลยี Facial Recognition มาใช้กับธุรกรรมเปิดบัญชี โอนเงิน เปลี่ยนเบอร์โทรศัพท์ และปรับเพิ่มวงเงินโอนต่อวัน โดยกำหนดค่า Face Comparison Threshold และใช้ประเภทของภาพใบหน้าอ้างอิง ดังนี้

ประเภทธุรกรรม	**ค่า Face Comparison Threshold**	**ประเภทของภาพใบหน้าอ้างอิง**
เปิดบัญชี	87	ภาพจากชิปบนบัตรประจำตัวประชาชน
โอนเงิน	80	ภาพ Selfie ที่จัดเก็บไว้ก่อนหน้า
เปลี่ยนเบอร์โทรศัพท์	87	ภาพ Selfie ที่จัดเก็บไว้ก่อนหน้า
ปรับเพิ่มวงเงินโอนต่อวัน	80	ภาพ Selfie ที่จัดเก็บไว้ก่อนหน้า

จากตัวอย่างข้างต้น ผู้ให้บริการต้องจัดให้มีการทดสอบ 3 ชุด เนื่องจากมีรูปแบบการตั้งค่าและประเภทของภาพใบหน้าอ้างอิงที่แตกต่างกัน 3 รูปแบบ โดยธุรกรรมโอนเงินและธุรกรรมปรับเพิ่มวงเงินโอนต่อวันใช้รูปแบบการตั้งค่าและประเภทของภาพใบหน้าอ้างอิงเหมือนกัน จึงสามารถใช้ผลการทดสอบชุดเดียวกันได้

ภาคผนวก ข กรอบการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection

ผู้ให้บริการต้องจัดให้มีการทดสอบนำเสนอสื่อโจมตีต่อเทคโนโลยี Facial Recognition ที่มีการใช้งานเทคโนโลยี Presentation Attack Detection โดยไม่แยกทดสอบเฉพาะเทคโนโลยี Presentation Attack Detection (PAD Subsystem) เพื่อให้ผลการทดสอบสะท้อนความสามารถของเทคโนโลยีในการตรวจจับและป้องกัน Presentation Attack ภายใต้สภาพการใช้งานจริง

การทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection แต่ละชุด ต้องเป็นไปตามข้อกำหนดขั้นต่ำดังต่อไปนี้

1. การตั้งค่าของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection

1.1 ทดสอบโดยใช้การตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและเทคโนโลยี Presentation Attack Detection เช่น ค่า Threshold และ Liveness Detection Setting รวมทั้งประเภทของภาพใบหน้าอ้างอิง ให้สอดคล้องกับการใช้งานจริง

1.2 ไม่เปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและเทคโนโลยี Presentation Attack Detection รวมทั้งประเภทของภาพใบหน้าอ้างอิง ตลอดการทดสอบ

2. จำนวนธุรกรรมทดสอบ การเลือกกลุ่มตัวอย่าง และสื่อที่ใช้ในการทดสอบ

2.1 ทดสอบด้วยจำนวนกลุ่มตัวอย่างที่เพียงพอสำหรับการประเมินประสิทธิภาพของเทคโนโลยี โดยสอดคล้องกับมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับโดยทั่วไป เช่น จำนวนกลุ่มตัวอย่างอย่างน้อย 15 ราย[5]

2.2 เลือกกลุ่มตัวอย่างให้สอดคล้องกับกลุ่มผู้ใช้บริการจริงหรือกลุ่มผู้ใช้บริการเป้าหมาย เช่น กรณีที่ผู้ใช้บริการส่วนใหญ่เป็นคนไทย กลุ่มตัวอย่างควรประกอบด้วยคนไทยในสัดส่วนไม่น้อยกว่าร้อยละ 80 ของจำนวนกลุ่มตัวอย่างทั้งหมด เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีภายใต้ลักษณะประชากรที่ใกล้เคียงกับผู้ใช้งานจริง และลดความคลาดเคลื่อนจากการใช้กลุ่มตัวอย่างที่ไม่สอดคล้องกับบริบทการใช้งาน

[5] อ้างอิงจำนวนกลุ่มตัวอย่างขั้นต่ำตาม FIDO Biometrics Requirements v4.0

2.3 เลือกกลุ่มตัวอย่างให้มีการกระจายตัวของเพศอย่างเหมาะสม เช่น เพศชายและเพศหญิงมีสัดส่วนอยู่ระหว่างร้อยละ 40 ถึง 60 ของจำนวนกลุ่มตัวอย่างทั้งหมด[6] เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีในการเปรียบเทียบภาพใบหน้าของผู้ใช้บริการทั้งเพศชายและเพศหญิง

2.4 เลือกกลุ่มตัวอย่างให้มีการกระจายตัวของช่วงอายุอย่างเหมาะสม เช่น กลุ่มตัวอย่างครอบคลุมช่วงอายุ 18–30 ปี 31–50 ปี และ 51–70 ปี โดยแต่ละช่วงอายุมีสัดส่วนอยู่ระหว่างร้อยละ 25 ถึง 40 ของจำนวนกลุ่มตัวอย่างทั้งหมด[7] เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีในการเปรียบเทียบภาพใบหน้าของผู้ใช้บริการในหลากหลายช่วงอายุ

2.5 เลือกใช้สื่อโจมตีให้มีความหลากหลายเพียงพอต่อการประเมินประสิทธิภาพของเทคโนโลยี โดยครอบคลุมสื่อโจมตีที่มีระดับความซับซ้อนแตกต่างกัน และสอดคล้องกับมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับโดยทั่วไป เช่น เลือกใช้สื่อโจมตีระดับความซับซ้อนต่ำอย่างน้อย 6 ประเภท (Species) และสื่อโจมตีระดับความซับซ้อนปานกลางอย่างน้อย 8 ประเภท[8]

ทั้งนี้ ควรเลือกสื่อโจมตีที่มีข้อมูลสนับสนุนว่าเคยถูกใช้ในการโจมตีจริง หรือเป็นเทคนิคการโจมตีรูปแบบใหม่ หรือมีแนวโน้มว่าจะสามารถใช้โจมตีได้สำเร็จ และควรทบทวนและปรับเปลี่ยนประเภทของสื่อโจมตีที่ใช้ในการทดสอบอย่างสม่ำเสมอ เพื่อให้การทดสอบครอบคลุมรูปแบบการโจมตีที่หลากหลายและสอดคล้องกับภัยคุกคามในปัจจุบัน

ตัวอย่างสื่อโจมตีในแต่ละระดับความซับซ้อน มีดังนี้

ระดับความซับซ้อน	**ตัวอย่างสื่อโจมตี**
ต่ำ	ภาพใบหน้าจาก Social Media ที่พิมพ์ด้วยเครื่องพิมพ์ Inkjet หรือ Laser ลงบนกระดาษชนิดต่าง ๆ
	ภาพใบหน้าจาก Social Media ที่แสดงบนหน้าจอโทรศัพท์มือถือ แท็บเล็ต หรือคอมพิวเตอร์รุ่นต่าง ๆ
	วิดีโอจาก Social Media ที่แสดงบนหน้าจอโทรศัพท์มือถือ แท็บเล็ต หรือคอมพิวเตอร์รุ่นต่าง ๆ

[6] อ้างอิงสัดส่วนการกระจายตัวของเพศตาม ISO/IEC 19795-5

[7] อ้างอิงสัดส่วนการกระจายตัวของช่วงอายุตาม ISO/IEC 19795-5

[8] อ้างอิงจำนวน PAI Species ตาม FIDO Biometrics Requirements v4.0

	วิดีโอ Deepfake ที่สร้างจากภาพนิ่งเพียงภาพเดียว
ปานกลาง	วิดีโอที่มีการเคลื่อนไหวใบหน้าตามคำสั่งของเทคโนโลยี Liveness Detection และแสดงบนหน้าจอโทรศัพท์มือถือ แท็บเล็ต หรือคอมพิวเตอร์รุ่นต่าง ๆ
	หน้ากากกระดาษที่จัดทำจากภาพถ่ายความละเอียดสูง
	วิดีโอ Deepfake ที่สร้างจากภาพหลายภาพหรือวิดีโอของบุคคล เพื่อให้มีความสมจริงมากขึ้น
สูง	หน้ากากที่ทำจากเซรามิก ซิลิโคน หรือหน้ากากที่ใช้ในการแสดงละคร
	ใบหน้าที่สร้างด้วยเครื่องพิมพ์ 3 มิติ (3D Printed Faces) หรือหุ่นจำลองใบหน้าที่มีสีและพื้นผิวเสมือนจริง

ทั้งนี้ ให้ถือว่าสื่อโจมตีเป็นคนละประเภท เมื่อมีความแตกต่างในสาระสำคัญของสื่อโจมตี เช่น วัสดุที่ใช้จัดทำ หรืออุปกรณ์ที่ใช้แสดงผล รวมทั้งให้ถือว่าการใช้ภาพนิ่งและวิดีโอเป็นสื่อโจมตีคนละประเภท อย่างไรก็ตาม การใช้เครื่องมือหรือซอฟต์แวร์ที่แตกต่างกันในการผลิตสื่อโจมตี แต่สื่อโจมตีที่ได้มีลักษณะไม่แตกต่างกันอย่างมีนัยสำคัญ ให้ถือว่าเป็นสื่อโจมตีประเภทเดียวกัน เช่น การใช้โปรแกรม Video Call ที่แตกต่างกัน

นอกเหนือจากการเลือกสื่อโจมตีตามหลักการข้างต้น ผู้ให้บริการต้องจัดให้มีการนำสื่อโจมตีประเภทต่อไปนี้มาทดสอบเป็นอย่างน้อย

(1) วิดีโอ Deepfake ที่แสดงบนจอ Monitor ความละเอียดอย่างน้อย 3,840 × 2,160 พิกเซล ซึ่งใช้เทคโนโลยี QD-OLED และมีคุณสมบัติ Glare Free หรืออุปกรณ์แสดงผลที่มีคุณสมบัติเทียบเท่า โดยให้นับเป็นหนึ่งประเภทของสื่อโจมตีระดับความซับซ้อนต่ำหรือปานกลาง ขึ้นอยู่กับลักษณะของเครื่องมือที่ใช้สร้างวิดีโอ Deepfake ว่าใช้ภาพนิ่งเพียงภาพเดียว หรือใช้ภาพหลายภาพหรือวิดีโอของบุคคล

(2) วิดีโอ Live Stream ใบหน้าที่แสดงบนจอ Monitor ความละเอียดอย่างน้อย 3,840 × 2,160 พิกเซล ซึ่งใช้เทคโนโลยี QD-OLED และมีคุณสมบัติ Glare Free หรืออุปกรณ์แสดงผลที่มีคุณสมบัติเทียบเท่า โดยให้นับเป็นหนึ่งประเภทของสื่อโจมตีระดับความซับซ้อนปานกลาง

2.6 สำหรับสื่อโจมตีแต่ละประเภท ต้องจัดทำสื่อโจมตีจากบุคคลที่แตกต่างกันให้ครบตามจำนวนกลุ่มตัวอย่างที่ใช้ในการทดสอบ เช่น หากใช้กลุ่มตัวอย่าง 15 ราย ต้องจัดทำสื่อโจมตีอย่างน้อย 15 ชิ้นต่อประเภท

2.7 นำสื่อโจมตีแต่ละชิ้นมาใช้ในการทดสอบด้วยจำนวนธุรกรรมที่เพียงพอต่อการประเมินประสิทธิภาพของเทคโนโลยี และสอดคล้องกับมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับโดยทั่วไป เช่น นำสื่อโจมตีแต่ละชิ้นมาใช้ในการทดสอบอย่างน้อย 10 ธุรกรรมทดสอบ[9] ดังนั้น กรณีที่มีสื่อโจมตี 15 ชิ้นต่อประเภท จะมีธุรกรรมทดสอบอย่างน้อย 150 ธุรกรรมต่อสื่อโจมตีแต่ละประเภท

2.8 ตรวจสอบคุณภาพของสื่อโจมตีทุกชิ้นก่อนนำมาใช้ในการทดสอบ เพื่อให้มั่นใจว่าสื่อโจมตีสามารถแสดงใบหน้าได้อย่างมีคุณภาพเพียงพอสำหรับการประเมินประสิทธิภาพของเทคโนโลยี Presentation Attack Detection โดยอาจนำสื่อโจมตีไปทดสอบกับเทคโนโลยี Facial Recognition ที่ปิดการใช้งานเทคโนโลยี Presentation Attack Detection ซึ่งเทคโนโลยี Facial Recognition ดังกล่าวต้องสามารถเปรียบเทียบและระบุได้ว่าใบหน้าที่นำเสนอผ่านสื่อโจมตีเป็นบุคคลเดียวกันกับภาพใบหน้าอ้างอิง

3. ผู้ดำเนินการทดสอบ

3.1 ผู้ดำเนินการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection ควรมีความรู้ ความเข้าใจ และประสบการณ์ในการสร้างหรือใช้งานสื่อโจมตี รวมทั้งมีความเข้าใจเทคโนโลยี Presentation Attack Detection

4. อุปกรณ์ที่ติดตั้งเทคโนโลยี Presentation Attack Detection

4.1 ใช้เทคโนโลยี Presentation Attack Detection บนระบบปฏิบัติการเพียงหนึ่งระบบปฏิบัติการตลอดการทดสอบ โดยอาจใช้อุปกรณ์เคลื่อนที่ที่มีเวอร์ชันของระบบปฏิบัติการแตกต่างกันได้ ทั้งนี้ ควรใช้อุปกรณ์หลายรุ่นและหลายระดับ (Tier) เพื่อให้ผลการทดสอบสะท้อนประสิทธิภาพของเทคโนโลยีบนอุปกรณ์ที่หลากหลาย

5. ผลการทดสอบ

5.1 คำนวณค่า IAPAR สำหรับสื่อโจมตีแต่ละประเภทจากสูตร:

[9] อ้างอิงจำนวนตาม FIDO Biometrics Requirements v4.0

$$\text{IAPAR} = \left(\frac{\text{จำนวนธุรกรรมทดสอบที่เทคโนโลยีไม่สามารถตรวจจับสื่อโจมตี จนเกิดการตัดสินว่าใบหน้าที่นำเสนอผ่านสื่อโจมตีเป็นบุคคลเดียวกันกับภาพใบหน้าอ้างอิง}}{\text{จำนวนธุรกรรมทดสอบด้วยสื่อโจมตีทั้งหมด}} \right) \times 100$$

<u>ตัวอย่างการคำนวณ</u> ทดสอบนำเสนอสื่อโจมตีประเภท “วิดีโอ Deepfake ที่แสดงบนจอ Monitor รุ่น XX” จำนวน 150 ธุรกรรมทดสอบ และพบว่าเทคโนโลยีไม่สามารถตรวจจับสื่อโจมตี จนเกิดการตัดสินว่าใบหน้าที่นำเสนอผ่านสื่อโจมตีเป็นบุคคลเดียวกันกับภาพใบหน้าอ้างอิงจำนวน 5 ธุรกรรมทดสอบ ดังนั้น IAPAR สำหรับสื่อโจมตีประเภทนี้ = $\left(\frac{5}{150}\right) \times 100 = 3.33\%$

ในกรณีที่ผู้ให้บริการนำเทคโนโลยี Presentation Attack Detection มาใช้กับหลายประเภทธุรกรรม เช่น การเปิดบัญชีและการโอนเงิน และมีการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี Presentation Attack Detection เช่น Liveness Detection Threshold หรือ Liveness Detection Setting แตกต่างกันในแต่ละประเภทธุรกรรม ผู้ให้บริการต้องจัดให้มีการทดสอบแยกตามแต่ละรูปแบบการตั้งค่า

นอกจากนี้ กรณีที่ผู้ให้บริการนำเทคโนโลยี Presentation Attack Detection มาให้บริการบนหลายระบบปฏิบัติการ (Operating System) ผู้ให้บริการต้องจัดให้มีการทดสอบแยกตามแต่ละระบบปฏิบัติการ

ทั้งนี้ ในการทดสอบแต่ละชุด ต้องใช้การตั้งค่าเพียงหนึ่งรูปแบบ และใช้เทคโนโลยี Presentation Attack Detection บนระบบปฏิบัติการเพียงหนึ่งระบบปฏิบัติการตลอดการทดสอบ

<u>ตัวอย่าง</u> ผู้ให้บริการนำเทคโนโลยี Presentation Attack Detection มาให้บริการบนระบบปฏิบัติการ iOS และ Android สำหรับธุรกรรมเปิดบัญชี โอนเงิน เปลี่ยนเบอร์โทรศัพท์ และปรับเพิ่มวงเงินโอนต่อวัน โดยกำหนด Liveness Detection Threshold และ Liveness Detection Setting ดังนี้

ประเภทธุรกรรม	**Liveness Detection Threshold**	**Liveness Detection Setting**
เปิดบัญชี	90	แบบ Active และมี 3 Challenge-Response Actions

โอนเงิน	87	แบบ Passive
เปลี่ยนเบอร์โทรศัพท์	90	แบบ Active และมี 2 Challenge-Response Actions
ปรับเพิ่มวงเงินโอนต่อวัน	87	แบบ Passive

จากตัวอย่างข้างต้น ผู้ให้บริการต้องจัดให้มีการทดสอบ 3 ชุดต่อระบบปฏิบัติการ เนื่องจากมีรูปแบบการตั้งค่าที่แตกต่างกัน 3 รูปแบบ ดังนั้น กรณีที่ผู้ให้บริการนำเทคโนโลยี Presentation Attack Detection มาให้บริการบนระบบปฏิบัติการ iOS และ Android ผู้ให้บริการต้องจัดให้มีการทดสอบรวม 6 ชุด

เอกสารแนบ 1

แบบฟอร์มรายงานผลการทดสอบประสิทธิภาพของการเปรียบเทียบภาพใบหน้า (Face Comparison)

<u>คำชี้แจง:</u>
1. จัดให้มีการทดสอบแยกตามแต่ละรูปแบบการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและประเภทของภาพใบหน้าอ้างอิง โดยในการทดสอบแต่ละชุด ต้องใช้การตั้งค่าเพียงหนึ่งรูปแบบ และใช้ภาพใบหน้าอ้างอิงเพียงหนึ่งประเภทตลอดการทดสอบ
2. รายงานผลการทดสอบโดยใช้แบบฟอร์มหนึ่งแบบฟอร์มต่อการทดสอบหนึ่งชุด
3. ในกรณีที่ผู้ให้บริการมีผลการทดสอบจากบริษัทผู้พัฒนาเทคโนโลยี ผู้ให้บริการเทคโนโลยี หรือผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน ผู้ให้บริการอาจนำผลดังกล่าวมารายงานได้ หากเป็นไปตามเงื่อนไขดังต่อไปนี้

   3.1 ผลการทดสอบมีอายุไม่เกิน 1 ปี

   3.2 ข้อกำหนดการทดสอบสอดคล้องตามกรอบการทดสอบที่กำหนดในแนวปฏิบัติฉบับนี้

   ทั้งนี้ หากข้อกำหนดการทดสอบยังไม่ครบถ้วนตามที่กำหนดในแนวปฏิบัติฉบับนี้ ผู้ให้บริการต้องจัดให้มีการทดสอบเพิ่มเติมในส่วนที่ยังไม่ครบถ้วน

หัวข้อ	คำตอบ
1. ข้อมูลทั่วไป	
1.1 ชื่อผู้ให้บริการ	<u>*ตัวอย่าง*</u> *ธนาคาร ...../ บริษัท .....*
1.2 ประเภทธุรกรรมที่นำเทคโนโลยี Facial Recognition มาใช้	☐ เปิดบัญชีแบบ Face-to-Face ☐ เปิดบัญชีแบบ Non-Face-to-Face ☐ โอนเงินตั้งแต่ 50,000 บาทขึ้นไปต่อครั้ง ☐ โอนเงินมูลค่ารวมสะสมครบทุก 200,000 บาทในระยะเวลา 1 วัน ☐ ปรับเพิ่มวงเงินโอนต่อวัน ให้โอนได้ตั้งแต่ 50,000 บาทขึ้นไป ☐ อื่น ๆ (โปรดระบุ) .....

1.3 ประเภทของภาพใบหน้าที่ใช้ในการใช้งานจริง	○ ภาพ Selfie เทียบกับภาพ Selfie ที่จัดเก็บไว้ก่อนหน้า ○ ภาพ Selfie เทียบกับภาพจากชิปบนบัตรประจำตัวประชาชน ○ ภาพ Selfie เทียบกับภาพจากชิปในหนังสือเดินทางที่อ่านผ่าน NFC ○ ภาพ Selfie เทียบกับภาพบนบัตรประจำตัวประชาชน ○ อื่น ๆ (โปรดระบุ) .....
1.4 ชื่อหน่วยงานผู้ดำเนินการทดสอบ *(เช่น หน่วยงานภายในของผู้ให้บริการ บริษัทผู้พัฒนาเทคโนโลยี ห้องปฏิบัติการหรือบริษัททดสอบอิสระ ทั้งนี้ กรณีที่ผู้ให้บริการดำเนินการทดสอบเอง โปรดระบุชื่อหน่วยงานภายในที่ดำเนินการทดสอบ)*	*<u>ตัวอย่าง</u>* *ธนาคาร ..... ฝ่าย ...../ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ / บริษัท รับทดสอบ จำกัด*
1.5 วันที่เริ่มการทดสอบ	
1.6 วันที่สิ้นสุดการทดสอบ	
2. ข้อมูลเทคโนโลยี Facial Recognition ที่นำมาใช้และทดสอบ	
2.1 ชื่อเทคโนโลยี	
2.2 เวอร์ชันของเทคโนโลยี	
2.3 ชื่อบริษัทผู้พัฒนาเทคโนโลยี	
2.4 รูปแบบการติดตั้ง	☐ ติดตั้งและใช้งานแบบ On-Premises ☐ ติดตั้งและใช้งานบน Cloud Computing ☐ ใช้บริการเทคโนโลยี Facial Recognition แบบ Software as a Service จากผู้ให้บริการเทคโนโลยี ☐ ใช้บริการจากผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน เช่น IdP, e-KYC Provider

	☐ อื่น ๆ (โปรดระบุ) .....
2.5 รูปแบบการเชื่อมต่อ	☐ Software Development Kit (SDK) ☐ Application Programming Interface (API) ☐ อื่น ๆ (โปรดระบุ) .....
3. ข้อมูลการได้รับการประเมินตามมาตรฐานสากล (ถ้ามี)	
3.1 ชื่อมาตรฐาน	☐ ISO/IEC 19795 ☐ อื่น ๆ (โปรดระบุ) .....
3.2 ชื่อองค์กรหรือผู้เชี่ยวชาญที่ทำการประเมิน	*ตัวอย่าง* *BixeLab*
3.3 เวอร์ชันของเทคโนโลยีที่ได้รับการประเมิน	
4. ข้อมูลการตั้งค่าของเทคโนโลยี Facial Recognition	
4.1 ค่า Face Comparison Threshold	○ ผู้ให้บริการสามารถกำหนดหรือเปลี่ยนแปลงค่า Face Comparison Threshold เองได้ โปรดระบุค่า Face Comparison Threshold ที่ใช้ในการใช้งานจริงและในการทดสอบ ..... ○ ผู้ให้บริการไม่สามารถกำหนดหรือเปลี่ยนแปลงค่า Face Comparison Threshold เองได้
4.2 ทดสอบโดยใช้การตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าสอดคล้องกับการใช้งานจริง	○ ใช่ ○ ไม่ใช่
4.3 ไม่เปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าตลอดการทดสอบ	○ ใช่ ○ ไม่ใช่
5. จำนวนธุรกรรมทดสอบ การเลือกกลุ่มตัวอย่าง และสื่อที่ใช้ในการทดสอบ	

5.1 จำนวนธุรกรรมทดสอบ	*ตัวอย่าง* *300,700 ธุรกรรม*
5.2 จำนวนกลุ่มตัวอย่าง	*ตัวอย่าง* *776 ราย*
5.3 สัดส่วนเชื้อชาติของกลุ่มตัวอย่าง	*ตัวอย่าง* ● *ไทย 96%* ● *จีน 4%*
5.4 สัดส่วนเพศของกลุ่มตัวอย่าง	*ตัวอย่าง* ● *ชาย 55%* ● *หญิง 45%*
5.5 สัดส่วนอายุของกลุ่มตัวอย่าง	*ตัวอย่าง* ● *ช่วงอายุ 18-30 ปี 35%* ● *ช่วงอายุ 31-50 ปี 40%* ● *ช่วงอายุ 51-70 ปี 25%*
5.6 ภาพใบหน้าที่ใช้ในการทดสอบเป็นไปตามเกณฑ์คุณภาพที่กำหนดไว้	○ ใช่ ○ ไม่ใช่
5.7 ประเภทของภาพใบหน้าที่ใช้ในการทดสอบสอดคล้องกับประเภทของภาพใบหน้าที่ใช้ในการใช้งานจริง	○ ใช่ ○ ไม่ใช่

(เช่น กรณีที่การใช้งานจริงเป็นการเปรียบเทียบภาพ Selfie กับภาพจากชิปบนบัตรประจำตัวประชาชน ผู้ให้บริการต้องจัดให้มีการทดสอบด้วยการเปรียบเทียบภาพในรูปแบบเดียวกัน)	
6. ผลการทดสอบ	
6.1 ค่า False Match Rate (FMR)	*ตัวอย่าง* 0.007%

ร่าง

เอกสารแนบ 2

แบบฟอร์มรายงานผลการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection

<u>คำชี้แจง:</u>
1. จัดให้มีการทดสอบแยกตามแต่ละรูปแบบการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี Presentation Attack Detection และแยกตามแต่ละระบบปฏิบัติการ โดยในการทดสอบแต่ละชุด ต้องใช้การตั้งค่าเพียงหนึ่งรูปแบบ และใช้เทคโนโลยี Presentation Attack Detection บนระบบปฏิบัติการเพียงหนึ่งระบบปฏิบัติการตลอดการทดสอบ
2. รายงานผลการทดสอบโดยใช้แบบฟอร์มหนึ่งแบบฟอร์มต่อการทดสอบหนึ่งชุด
3. ในกรณีที่ผู้ให้บริการมีผลการทดสอบจากบริษัทผู้พัฒนาเทคโนโลยี ผู้ให้บริการเทคโนโลยี หรือผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน ผู้ให้บริการอาจนำผลดังกล่าวมารายงานได้ หากเป็นไปตามเงื่อนไขดังต่อไปนี้

   3.1 ผลการทดสอบมีอายุไม่เกิน 1 ปี

   3.2 ข้อกำหนดการทดสอบสอดคล้องตามกรอบการทดสอบที่กำหนดในแนวปฏิบัติฉบับนี้

   ทั้งนี้ หากข้อกำหนดการทดสอบยังไม่ครบถ้วนตามที่กำหนดในแนวปฏิบัติฉบับนี้ ผู้ให้บริการต้องจัดให้มีการทดสอบเพิ่มเติมในส่วนที่ยังไม่ครบถ้วน

หัวข้อ	คำตอบ
1. ข้อมูลทั่วไป	
1.1 ชื่อผู้ให้บริการ	<u>*ตัวอย่าง*</u> *ธนาคาร ...../ บริษัท .....*
1.2 ประเภทธุรกรรมที่นำเทคโนโลยี Presentation Attack Detection มาใช้	☐ เปิดบัญชีแบบ Face-to-Face ☐ เปิดบัญชีแบบ Non-Face-to-Face ☐ โอนเงินตั้งแต่ 50,000 บาทขึ้นไป ☐ โอนเงินมูลค่ารวมสะสมครบทุก 200,000 บาทในระยะเวลา 1 วัน ☐ ปรับเพิ่มวงเงินโอนต่อวัน ให้โอนได้ตั้งแต่ 50,000 บาทขึ้นไป ☐ อื่น ๆ (โปรดระบุ) .....

1.3 ชื่อหน่วยงานผู้ดำเนินการทดสอบ *(เช่น หน่วยงานภายในของผู้ให้บริการ บริษัทผู้พัฒนาเทคโนโลยี ห้องปฏิบัติการหรือบริษัททดสอบอิสระ ทั้งนี้ กรณีที่ผู้ให้บริการดำเนินการทดสอบเอง โปรดระบุชื่อหน่วยงานภายในที่ดำเนินการทดสอบ)*	*<u>ตัวอย่าง</u>* *ธนาคาร ..... ฝ่าย ...../ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ / บริษัท รับทดสอบ จำกัด*
1.4 วันที่เริ่มการทดสอบ	
1.5 วันที่สิ้นสุดการทดสอบ	
2. ข้อมูลเทคโนโลยี Presentation Attack Detection ที่นำมาใช้และทดสอบ	
2.1 ชื่อเทคโนโลยี	
2.2 เวอร์ชันของเทคโนโลยี	
2.3 ชื่อบริษัทผู้พัฒนาเทคโนโลยี	
2.4 รูปแบบการติดตั้ง	☐ ติดตั้งและใช้งานแบบ On-Premises ☐ ติดตั้งและใช้งานบน Cloud Computing ☐ ใช้บริการเทคโนโลยี Presentation Attack Detection แบบ Software as a Service จากผู้ให้บริการเทคโนโลยี ☐ ใช้บริการจากผู้ให้บริการด้านการพิสูจน์หรือยืนยันตัวตน เช่น IdP, e-KYC Provider ☐ อื่น ๆ (โปรดระบุ) .....
2.5 รูปแบบการเชื่อมต่อ	☐ Software Development Kit (SDK) ☐ Application Programming Interface (API) ☐ อื่น ๆ (โปรดระบุ) .....
3. ข้อมูลการได้รับการประเมินตามมาตรฐานสากล (ถ้ามี)	

3.1 ชื่อมาตรฐาน	☐ ISO/IEC 30107 ☐ อื่น ๆ (โปรดระบุ) .....
3.2 ชื่อองค์กรหรือผู้เชี่ยวชาญที่ทำการประเมิน	*ตัวอย่าง* *iBeta/BixeLab*
3.3 เวอร์ชันของเทคโนโลยีที่ได้รับการประเมิน	
3.4 ประเภทของเทคโนโลยี Presentation Attack Detection ที่ได้รับการประเมิน	☐ Presentation Attack Detection ที่ไม่ใช่ Liveness Detection ☐ Active Liveness Detection ☐ Passive Liveness Detection ☐ Liveness Detection ประเภทอื่น (โปรดระบุ) .....
3.5 ระดับของการทดสอบที่ผ่านการประเมิน	☐ PAD Level 1 ☐ PAD Level 2 ☐ PAD Level 3 ☐ อื่น ๆ (โปรดระบุ) .....
4. ข้อมูลการตั้งค่าของเทคโนโลยี Presentation Attack Detection	
4.1 ประเภทของเทคโนโลยี Presentation Attack Detection ที่ใช้ในการใช้งานจริงและในการทดสอบ	☐ Presentation Attack Detection ที่ไม่ใช่ Liveness Detection ☐ Active Liveness Detection ☐ Passive Liveness Detection ☐ Liveness Detection ประเภทอื่น (โปรดระบุ) .....

Draft

4.2 กรณีที่ใช้เทคโนโลยี Liveness Detection แบบ Active โปรดระบุจำนวนและรายละเอียดของ Challenge-Response Actions ที่ใช้ในการใช้งานจริงและในการทดสอบ	*<u>ตัวอย่าง</u>* *4 Actions ได้แก่* *1. อ้าปาก* *2. กระพริบตา* *3. สุ่มระหว่าง หันซ้ายและหันขวา* *4. color flashing สีแดง สีน้ำเงิน และสีเขียว*
4.3 ค่า Liveness Detection Threshold / Presentation Attack Detection Threshold	❍ ผู้ให้บริการสามารถกำหนดหรือเปลี่ยนแปลงค่า Liveness Detection Threshold / Presentation Attack Detection Threshold เองได้ โปรดระบุค่า Liveness Detection Threshold / Presentation Attack Detection Threshold ที่ใช้ในการใช้งานจริงและในการทดสอบ ..... ❍ ผู้ให้บริการไม่สามารถกำหนดหรือเปลี่ยนแปลงค่า Liveness Detection Threshold / Presentation Attack Detection Threshold เองได้
4.4 ทดสอบโดยใช้การตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและเทคโนโลยี Presentation Attack Detection รวมทั้งประเภทของภาพใบหน้าอ้างอิง สอดคล้องกับการใช้งานจริง	❍ ใช่ ❍ ไม่ใช่
4.5 ไม่เปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของการเปรียบเทียบภาพใบหน้าและเทคโนโลยี Presentation Attack Detection รวมทั้งประเภทของภาพใบหน้าอ้างอิง ตลอดการทดสอบ	❍ ใช่ ❍ ไม่ใช่
5. จำนวนธุรกรรมทดสอบ การเลือกกลุ่มตัวอย่าง และสื่อที่ใช้ในการทดสอบ	

Draft

5.1 จำนวนกลุ่มตัวอย่าง *(กรณีที่จำนวนกลุ่มตัวอย่างน้อยกว่า 15 ราย โปรดระบุมาตรฐานสากลหรือแนวปฏิบัติที่ใช้อ้างอิง)*	*<u>ตัวอย่าง</u>* *15 ราย*
5.2 สัดส่วนเชื้อชาติของกลุ่มตัวอย่าง	*<u>ตัวอย่าง</u>* ● *ไทย 87%* ● *จีน 13%*
5.3 สัดส่วนเพศของกลุ่มตัวอย่าง	*<u>ตัวอย่าง</u>* ● *ชาย 53%* ● *หญิง 47%*
5.4 สัดส่วนอายุของกลุ่มตัวอย่าง	*<u>ตัวอย่าง</u>* *ช่วงอายุ 18-30 ปี 35%* *ช่วงอายุ 31-50 ปี 40%* *ช่วงอายุ 51-70 ปี 25%*
5.5 สื่อโจมตีระดับความซับซ้อนต่ำทุกประเภทที่ใช้ในการทดสอบ *(กรณีที่จำนวนประเภทของสื่อโจมตีระดับความซับซ้อนต่ำที่ใช้ในการทดสอบน้อยกว่า 6 ประเภท โปรดระบุมาตรฐานสากลหรือแนวปฏิบัติที่ใช้อ้างอิง)*	*<u>ตัวอย่าง</u>* ● *ประเภทที่ 1: ภาพใบหน้าจาก Social Media ของกลุ่มตัวอย่างที่พิมพ์บนกระดาษ A4 ด้วยเครื่องพิมพ์เลเซอร์ Brother HL-L6200DW* ● *ประเภทที่ 2: ภาพใบหน้าของกลุ่มตัวอย่างที่ดาวน์โหลดจากเว็บไซต์ และนำมาแสดงบนโทรศัพท์มือถือ iPhone 16 Pro Max*

	● *ประเภทที่ 3: วิดีโอจาก Social Media ของกลุ่มตัวอย่างที่แสดงบนจอ Monitor รุ่น Samsung Odyssey OLED G8* ● *ประเภทที่ 4: วิดีโอจาก Social Media ของกลุ่มตัวอย่างที่แสดงบนโทรศัพท์มือถือ Samsung Galaxy S25 Ultra* ● *ประเภทที่ 5: วิดีโอ Live Stream Deepfake ที่สร้างด้วยโปรแกรม DeepFaceLive โดยใช้ภาพใบหน้าของกลุ่มตัวอย่างเพียง 1 ภาพ และแสดงบนจอ Monitor รุ่น ASUS ROG Swift OLED PG32UCDM* ● *ประเภทที่ 6: วิดีโอ Live Stream Deepfake ที่สร้างด้วยโปรแกรม Picsi.AI โดยใช้ภาพใบหน้าของกลุ่มตัวอย่างเพียง 1 ภาพ และแสดงบนจอ Monitor รุ่น Samsung Odyssey OLED G8*
5.6 สื่อโจมตีระดับความซับซ้อนปานกลางทุกประเภทที่ใช้ในการทดสอบ *(กรณีที่จำนวนประเภทของสื่อโจมตีระดับความซับซ้อนปานกลางที่ใช้ในการทดสอบน้อยกว่า 8 ประเภท โปรดระบุมาตรฐานสากลหรือแนวปฏิบัติที่ใช้อ้างอิง)*	*<u>ตัวอย่าง</u>* ● *ประเภทที่ 1: วิดีโอที่บันทึกการเคลื่อนไหวใบหน้าของกลุ่มตัวอย่าง เช่น อ้าปาก หันซ้าย หันขวา ไว้ล่วงหน้า และนำมาแสดงบน Samsung Galaxy Tab S10 Ultra* ● *ประเภทที่ 2: วิดีโอที่บันทึกการเคลื่อนไหวใบหน้าของกลุ่มตัวอย่างไว้ล่วงหน้า และนำมาแสดงบนคอมพิวเตอร์ ASUS Zen AiO 24* ● *ประเภทที่ 3: วิดีโอ Live Stream ใบหน้าของกลุ่มตัวอย่างที่แสดงบนจอ Monitor รุ่น Samsung Odyssey OLED G8* ● *ประเภทที่ 4: วิดีโอ Live Stream ใบหน้าของกลุ่มตัวอย่างที่แสดงบน Apple iPad Pro 13* ● *ประเภทที่ 5: วิดีโอ Live Stream ใบหน้าของกลุ่มตัวอย่างที่แสดงบนโทรศัพท์มือถือ OnePlus 9 Pro*

2019

	● *ประเภทที่ 6: วิดีโอ Live Stream ใบหน้าของกลุ่มตัวอย่างที่แสดงบนจอ Monitor รุ่น ASUS ROG Swift OLED PG32UCDM* ● *ประเภทที่ 7: วิดีโอ Live Stream ใบหน้าของกลุ่มตัวอย่างที่แสดงบนโทรศัพท์มือถือ iPhone 16 Pro Max* ● *ประเภทที่ 8: หน้ากากกระดาษที่จัดทำจากภาพถ่ายความละเอียดสูงของกลุ่มตัวอย่าง โดยตัดบริเวณดวงตาออก*
5.7 สื่อโจมตีระดับความซับซ้อนสูงทุกประเภทที่ใช้ในการทดสอบ (ถ้ามี)	<u>*ตัวอย่าง*</u> ● *ประเภทที่ 1 : หน้ากากซิลิโคนที่เลียนแบบใบหน้าของกลุ่มตัวอย่าง* ● *ประเภทที่ 2 : หน้ากากเซรามิกที่เลียนแบบใบหน้าของกลุ่มตัวอย่าง*
5.8 จำนวนสื่อโจมตีต่อสื่อโจมตีแต่ละประเภท	<u>*ตัวอย่าง*</u> *15 ชิ้นต่อประเภท ยกเว้นสื่อโจมตีระดับความซับซ้อนสูงที่มีประเภทละ 1 ชิ้น*
5.9 จำนวนธุรกรรมทดสอบต่อสื่อโจมตีแต่ละชิ้น *(กรณีที่จำนวนธุรกรรมทดสอบต่อสื่อโจมตีแต่ละชิ้นน้อยกว่า 10 ธุรกรรม โปรดระบุมาตรฐานสากลหรือแนวปฏิบัติที่ใช้อ้างอิง)*	<u>*ตัวอย่าง*</u> *10 ธุรกรรมต่อชิ้น ยกเว้นสื่อโจมตีระดับความซับซ้อนสูงที่ทดสอบชิ้นละ 20 ธุรกรรม*
5.10 ตรวจสอบคุณภาพของสื่อโจมตีทุกชิ้นก่อนนำมาใช้ในการทดสอบ	○ ใช่ ○ ไม่ใช่
6. อุปกรณ์เคลื่อนที่ที่ติดตั้งเทคโนโลยี Presentation Attack Detection	
6.1 รุ่นของอุปกรณ์เคลื่อนที่ที่ติดตั้งเทคโนโลยี Presentation Attack Detection และใช้ในการทดสอบ พร้อมเวอร์ชันของระบบปฏิบัติการ	<u>*ตัวอย่าง*</u> *1. Samsung Galaxy A06: Android 10* *2. Google Pixel 8a: Android 11*

NIA

	3. Xiaomi 15 Ultra: Android 16
7. ผลการทดสอบ	
7.1 ค่า Impostor Attack Presentation Accept Rate (IAPAR) สำหรับสื่อโจมตีแต่ละประเภท	*<u>ตัวอย่าง</u>* *สื่อโจมตีระดับความซับซ้อนต่ำ* • *ประเภทที่ 1: 0%* • *ประเภทที่ 2: 0%* • *ประเภทที่ 3: 0%* • *ประเภทที่ 4: 0%* • *ประเภทที่ 5: 0%* • *ประเภทที่ 6: 0%* *สื่อโจมตีระดับความซับซ้อนปานกลาง* • *ประเภทที่ 1: 0%* • *ประเภทที่ 2: 0%* • *ประเภทที่ 3: 2.67%* • *ประเภทที่ 4: 0%* • *ประเภทที่ 5: 0%* • *ประเภทที่ 6: 0%* • *ประเภทที่ 7: 4%* • *ประเภทที่ 8: 3.33%*

	สื่อโจมตีระดับความซับซ้อนสูง • *ประเภทที่ 1: 0%* • *ประเภทที่ 2: 0%*

ร่าง

เอกสารแนบ 3

แบบฟอร์มรายงานผลการตรวจประเมินการปฏิบัติตามแนวปฏิบัติ

คำชี้แจง: การตรวจประเมินและจัดทำรายงานผลการตรวจประเมินการปฏิบัติตามแนวปฏิบัติ ให้ดำเนินการโดยหน่วยงานตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระ

ชื่อผู้ให้บริการ.....

ชื่อเทคโนโลยี Facial Recognition ที่นำมาใช้ใหม่.....

ชื่อเทคโนโลยี Presentation Attack Detection ที่นำมาใช้ใหม่.....

ชื่อบริษัทผู้ตรวจประเมิน.....

วันที่ตรวจประเมินแล้วเสร็จ.....

ลำดับที่	ประเด็นที่ต้องตรวจประเมิน	การปฏิบัติของผู้ให้บริการ
ส่วนที่ 1 การรักษาความมั่นคงปลอดภัยของระบบ		
อ้างอิงข้อ (2): กระบวนการบริหารจัดการ Security Patch		
1	*ระยะเวลา (SLA) ในการติดตั้ง Security Patch บนระบบที่ให้บริการจริงตามระดับความเสี่ยงของช่องโหว่*	
2	*กระบวนการขออนุมัติยกเว้นและประเมินความเสี่ยง กรณีที่ไม่สามารถติดตั้ง Security Patch ได้*	
อ้างอิงข้อ (3): Vulnerability Assessment		
3	*ความถี่ในการดำเนินการประเมินช่องโหว่*	

4	*ผลการประเมินช่องโหว่ครั้งล่าสุด*	
5	*ระยะเวลา (SLA) ในการปรับปรุงแก้ไขช่องโหว่ที่ตรวจพบ*	
6	*หน่วยงานหรือผู้รับผิดชอบในการติดตามการปรับปรุงแก้ไขช่องโหว่ที่ตรวจพบ*	
7	*คณะกรรมการหรือผู้บริหารที่ได้รับรายงานความคืบหน้าการดำเนินการปรับปรุงแก้ไขช่องโหว่ที่ตรวจพบ*	
อ้างอิงข้อ (4): Penetration Test		
8	*ความถี่ในการดำเนินการทดสอบเจาะระบบ*	
9	*หน่วยงานหรือผู้ดำเนินการทดสอบเจาะระบบครั้งล่าสุด*	
10	*ประเภทการโจมตีที่ใช้ในการทดสอบเจาะระบบครั้งล่าสุด (เช่น Presentation Attack, Video Injection Attack, การโจมตีผ่าน API)*	
11	*ความเป็นอิสระระหว่างผู้ดำเนินการทดสอบเจาะระบบด้วย Presentation Attack และผู้ดำเนินการทดสอบประสิทธิภาพของเทคโนโลยี Presentation Attack Detection*	
12	*ผลการทดสอบเจาะระบบครั้งล่าสุด*	
13	*ระยะเวลา (SLA) ในการปรับปรุงแก้ไข Finding ที่ตรวจพบ*	
14	*หน่วยงานหรือผู้รับผิดชอบในการติดตามการปรับปรุงแก้ไข Finding ที่ตรวจพบ*	
15	*คณะกรรมการหรือผู้บริหารที่ได้รับรายงานความคืบหน้าการดำเนินการปรับปรุงแก้ไข Finding ที่ตรวจพบ*	
อ้างอิงข้อ (5): การจัดเก็บ Log		
16	*เหตุการณ์ที่มีการจัดเก็บ Log (เช่น การเข้าถึง การสร้าง การแก้ไข และการลบข้อมูลชีวมิติ)*	
17	*มาตรการป้องกันการแก้ไขหรือทำลาย Log โดยไม่ได้รับอนุญาต*	

18	*ระยะเวลาการเก็บรักษา Log*	
ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติและการป้องกันการสวมรอย		
ส่วนที่ 2.1 การเก็บข้อมูลใบหน้าจากผู้ใช้บริการ (Face Data Capture)		
อ้างอิงข้อ (1): กลไกตรวจจับอุปกรณ์หรือสภาพแวดล้อมที่มีความเสี่ยง		
19	*กลไกหรือเครื่องมือตรวจจับการใช้งานเทคโนโลยี Facial Recognition บน Rooted/Jailbroken Device*	
20	*การตอบสนองเมื่อตรวจพบการใช้งานเทคโนโลยี Facial Recognition บน Rooted/Jailbroken Device*	
21	*ความถี่ในการทบทวนและปรับปรุงกลไกหรือเครื่องมือตรวจจับการใช้งานเทคโนโลยี Facial Recognition บน Rooted/Jailbroken Device*	
22	*กลไกหรือเครื่องมือตรวจจับการใช้งานเทคโนโลยี Facial Recognition บนอุปกรณ์หรือสภาพแวดล้อมที่จำลองการทำงานของอุปกรณ์จริง*	
23	*ประเภทของอุปกรณ์หรือสภาพแวดล้อมที่จำลองการทำงานของอุปกรณ์จริงที่กลไกหรือเครื่องมือสามารถตรวจจับได้ (เช่น Virtual Device, Emulator และ Simulator)*	
24	*การตอบสนองเมื่อตรวจพบการใช้งานเทคโนโลยี Facial Recognition บนอุปกรณ์หรือสภาพแวดล้อมที่จำลองการทำงานของอุปกรณ์จริง*	
25	*ความถี่ในการทบทวนและปรับปรุงกลไกหรือเครื่องมือตรวจจับการใช้งานเทคโนโลยี Facial Recognition บนอุปกรณ์หรือสภาพแวดล้อมที่จำลองการทำงานของอุปกรณ์จริง*	
อ้างอิงข้อ (2): กลไกป้องกัน Reverse Engineering		
26	*เทคนิคหรือเครื่องมือที่ใช้ในการทำ Code Obfuscation*	

27	*ขอบเขตการทำ Code Obfuscation (เช่น ครอบคลุมทั้งแอปพลิเคชัน หรือเฉพาะส่วนที่เกี่ยวข้องกับเทคโนโลยี Facial Recognition และ Presentation Attack Detection)*	
28	*ความถี่ในการทบทวนและปรับปรุงเทคนิคหรือเครื่องมือที่ใช้ในการทำ Code Obfuscation*	
อ้างอิงข้อ (3): กลไกตรวจจับการดัดแปลงหรือการแทรกแซงการทำงานของแอปพลิเคชัน		
29	*กลไกหรือเครื่องมือตรวจจับการดัดแปลงหรือการแทรกแซงการทำงานของแอปพลิเคชันที่ใช้เทคโนโลยี Facial Recognition*	
30	*ประเภทของการดัดแปลงหรือการแทรกแซงที่กลไกหรือเครื่องมือสามารถตรวจจับได้ (เช่น Anti-Tampering, Anti-Hooking, Anti-Debugging, Runtime Integrity Check หรือ SDK Integrity Check)*	
31	*การตอบสนองเมื่อตรวจพบการดัดแปลงหรือการแทรกแซงการทำงานของแอปพลิเคชันที่ใช้เทคโนโลยี Facial Recognition*	
32	*ความถี่ในการทบทวนและปรับปรุงกลไกหรือเครื่องมือตรวจจับการดัดแปลงหรือการแทรกแซงการทำงานของแอปพลิเคชันที่ใช้เทคโนโลยี Facial Recognition*	
อ้างอิงข้อ (7): เทคโนโลยี Presentation Attack Detection		
33	*การตอบสนองเมื่อตรวจพบการนำเสนอสื่อโจมตีต่อเทคโนโลยี Facial Recognition*	
อ้างอิงข้อ (8): กลไกป้องกัน Replay Attack		
34	*กลไกป้องกัน Replay Attack ระหว่างโมดูล Facial Recognition บนแอปพลิเคชันของผู้ใช้บริการกับระบบ Facial Recognition หรือระบบ Backend ของผู้ให้บริการ*	

35	*ระยะเวลาที่ Request หรือข้อมูลที่ใช้ในการพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition ที่รับส่งระหว่างโมดูล Facial Recognition บนแอปพลิเคชันของผู้ใช้บริการกับระบบ Facial Recognition หรือระบบ Backend ของผู้ให้บริการสามารถใช้งานได้*	
ส่วนที่ 2.2 การประมวลผลและการเก็บรักษาข้อมูลชีวมิติ (Signal Processing and Biometric Data Storage)		
อ้างอิงข้อ (1): การเก็บรักษาข้อมูลใบหน้า ข้อมูลอ้างอิงชีวมิติ และข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการแยกจากกัน		
36	*การแยกเก็บรักษาข้อมูลใบหน้า ข้อมูลอ้างอิงชีวมิติ และข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการ* (1) เก็บรักษาข้อมูลใบหน้า ข้อมูลอ้างอิงชีวมิติ และข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการที่จำเป็นต่อการทำงานของเทคโนโลยี Facial Recognition แยกจากกัน โดยอย่างน้อยต้องมีการแยกข้อมูลแบบ Logical Separation เช่น การ	
37	*การกำหนดสิทธิการเข้าถึงข้อมูลใบหน้า ข้อมูลอ้างอิงชีวมิติ และข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการ*	
38	*รูปแบบการเก็บรักษาข้อมูลใบหน้าของผู้ใช้บริการ (เช่น On-Premises, Private Cloud, Public Cloud)*	
อ้างอิงข้อ (2): Multi-Factor Authentication		
39	*วิธีการพิสูจน์ตัวตนแบบหลายปัจจัย (MFA) ที่ใช้สำหรับการเข้าถึงข้อมูลชีวมิติ และการกำหนดหรือเปลี่ยนแปลงการตั้งค่าที่อาจส่งผลกระทบต่อประสิทธิภาพของเทคโนโลยี Facial Recognition และเทคโนโลยี Presentation Attack Detection*	
40	*ความถี่ เงื่อนไขและกระบวนการทบทวนสิทธิการเข้าถึง*	
41	*กระบวนการขออนุมัติยกเว้นและประเมินความเสี่ยง กรณีที่ระบบไม่รองรับการพิสูจน์ตัวตนแบบหลายปัจจัย*	

อ้างอิงข้อ (3): การเข้ารหัสและตรวจสอบความถูกต้องครบถ้วน (Integrity) ของข้อมูลชีวมิติ		
42	*กลไก อัลกอริทึมและความยาวกุญแจเข้ารหัสที่ใช้เข้ารหัสข้อมูลชีวมิติขณะจัดเก็บ (Data at Rest)*	
43	*กลไกและอัลกอริทึมที่ใช้ตรวจสอบความถูกต้องครบถ้วน (Integrity) ของข้อมูลชีวมิติขณะจัดเก็บ (Data at Rest)*	
44	*กลไก อัลกอริทึมและความยาวกุญแจเข้ารหัสที่ใช้เข้ารหัสข้อมูลชีวมิติขณะรับส่งข้อมูล (Data in Transit)*	
45	*กลไกและอัลกอริทึมที่ใช้ตรวจสอบความถูกต้องครบถ้วน (Integrity) ของข้อมูลชีวมิติขณะรับส่งข้อมูล (Data in Transit)*	
46	*แนวทางการบริหารจัดการกุญแจเข้ารหัสตลอดวงจรชีวิต*	
อ้างอิงข้อ (4): การยกเลิกการใช้งานข้อมูลอ้างอิงชีวมิติเดิมและลงทะเบียนข้อมูลอ้างอิงชีวมิติใหม่		
47	*กระบวนการยกเลิกการใช้งานข้อมูลอ้างอิงชีวมิติเดิมและลงทะเบียนข้อมูลอ้างอิงชีวมิติใหม่*	
48	*ระยะเวลาหรือเงื่อนไขในการปรับปรุงข้อมูลอ้างอิงชีวมิติ*	
49	*วิธีการยืนยันตัวตนผู้ใช้บริการก่อนดำเนินการลงทะเบียนข้อมูลอ้างอิงชีวมิติใหม่*	
ส่วนที่ 2.3 การเปรียบเทียบภาพใบหน้าและการตัดสินผลการเปรียบเทียบภาพใบหน้า (Face Comparison and Decision)		
อ้างอิงข้อ (1): จำกัดการเปิดเผยผลการเปรียบเทียบภาพใบหน้า		
50	*ช่องทางที่มีการเปิดเผยผลการเปรียบเทียบภาพใบหน้า (เช่น API หรือ Log)*	
อ้างอิงข้อ (2): จำนวนครั้งสูงสุดที่ผู้ใช้บริการสามารถพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition แล้วไม่สำเร็จติดต่อกัน		
51	*จำนวนครั้งสูงสุดที่ผู้ใช้บริการสามารถพิสูจน์หรือยืนยันตัวตนด้วยเทคโนโลยี Facial Recognition แล้วไม่สำเร็จติดต่อกัน*	

52	*การตอบสนองเมื่อจำนวนครั้งที่ไม่สำเร็จติดต่อกันถึงเกณฑ์ที่กำหนด*	
ส่วนที่ 3 การรักษาประสิทธิภาพของเทคโนโลยี		
อ้างอิงข้อ (1): เกณฑ์ประสิทธิภาพของเทคโนโลยี		
53	*ประสิทธิภาพของเทคโนโลยี Facial Recognition (FMR) และ Presentation Attack Detection (IAPAR)*	
อ้างอิงข้อ (3): กระบวนการเฝ้าระวัง ตรวจสอบ และตอบสนองต่อเหตุการณ์		
54	*กระบวนการตอบสนองเมื่อพบความผิดปกติด้านประสิทธิภาพ เช่น ค่า FMR หรือค่า IAPAR สำหรับสื่อโจมตีประเภทใดประเภทหนึ่งเพิ่มขึ้นจนเกินเกณฑ์ประสิทธิภาพที่กำหนดไว้ และกรณีที่ได้รับข้อมูลเกี่ยวกับภัยคุกคาม ช่องโหว่ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อประสิทธิภาพหรือความมั่นคงปลอดภัยของเทคโนโลยี*	

Draft