ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 29 เล่ม 1-2565

# ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 1: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

# BIOMETRIC TECHNOLOGY – PART 1: BIOMETRIC TECHNOLOGY USAGE FOR PERSONAL VERIFICATION

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.240.15

# ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 1: การใช้งานเทคโนโลยีชีวมิติ สำหรับการพิสูจน์และยืนยันตัวตน

**ขมธอ. 29 เล่ม 1-2565**


**สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์**

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200



ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 21 เมษายน พ.ศ. 2565

## คณะทำงานจัดทำมาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ

**ที่ปรึกษาคณะทำงาน**

| | |
|---|---|
| ศาสตราจารย์ ดร.วุฒิพงศ์ อารีกุล | มหาวิทยาลัยเกษตรศาสตร์ |

**ประธานคณะทำงาน**

| | |
|---|---|
| นายชัยชนะ มิตรพันธ์ | สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ |

**คณะทำงาน**

| | |
|---|---|
| นางสมศรี หอกันยา | สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม |
| ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร | สำนักงานปลัดกระทรวงมหาดไทย |
| นายสัญชัย เตชนิมิตวัช | กรมการปกครอง |
| นายณัฏฐา พาชัยยุทธ | สำนักงานคณะกรรมการพัฒนาระบบราชการ |
| นางสาวอาจารีย์ ศุภพิโรจน์ | ธนาคารแห่งประเทศไทย |
| นายสมเกียรติ วัฒนาประสบสุข | สำนักงานคณะกรรมการกำกับและส่งเสริม การประกอบธุรกิจประกันภัย |
| นายวิบูลย์ ภัทรพิบูล | สำนักงานคณะกรรมการกำกับหลักทรัพย์ และตลาดหลักทรัพย์ |
| นายศุภกาญจน์ บุญจันทร์ | สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ |
| นายอาศิส อัญญะโพธิ์ | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) |
| ศาสตราจารย์ ดร.วิเชียร เปรมชัยสวัสดิ์ | สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย |
| นายสืบศักดิ์ สืบภักดี | สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ |
| นายยศ กิมสวัสดิ์ | สมาคมธนาคารไทย |
| นายณัฐพล โลหชิตพิทักษ์ | สมาคมบริษัทหลักทรัพย์ไทย |
| นายทำนุ อมาตยกุล | สมาคมประกันชีวิตไทย |
| นางสาวปิยกานต์ ญาณอุดม | สมาคมประกันวินาศภัยไทย |

**เลขานุการ**

| | |
|---|---|
| นายสมบัติ ชั้นอินทร์งาม | สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ |

**ผู้ช่วยเลขานุการ**

| | |
|---|---|
| นายธวัชชัย พริ้งพร้อม | สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ |

**วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ**
**ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 1: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน**


| | |
|---|---|
| ดร. อรุชา รุ่งโชคอนันต์ | มหาวิทยาลัยเกษตรศาสตร์ |
| ดร. กิตติพล โหราพงศ์ | มหาวิทยาลัยเกษตรศาสตร์ |
| นางสาวพลอยนภัส เกิดจิรโรจน์ | มหาวิทยาลัยเกษตรศาสตร์ |

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 1: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและข้อเสนอแนะสำหรับการบริหารจัดการอัตลักษณ์บุคคลจากการพิสูจน์และยืนยันตัวตนด้วยการใช้เทคโนโลยีชีวมิติ โดยมีเป้าหมายเพื่อให้มีการนำเทคโนโลยีชีวมิติไปประยุกต์ใช้กับการพิสูจน์และยืนยันตัวตนในภาคบริการประชาชนได้อย่างมีประสิทธิภาพสูงสุด มีความน่าเชื่อถือในระดับสากล มีความถูกต้องโปร่งใส มีความปลอดภัย และมีธรรมาภิบาล

ข้อเสนอแนะมาตรฐานนี้เหมาะกับหน่วยงานภาครัฐหรือภาคเอกชนที่ต้องการนำเทคโนโลยีชีวมิติไปประยุกต์ใช้งานในการพิสูจน์และยืนยันตัวตน ซึ่งเป็นส่วนหนึ่งของระบบบริหารจัดการอัตลักษณ์บุคคล (Identity Management System: IdMS) โดยข้อเสนอแนะมาตรฐานนี้ สามารถนำไปประยุกต์ใช้ในหน่วยงานที่เกี่ยวข้องกับการรักษาความปลอดภัยในหน่วยงานราชการหรือเอกชน รวมถึงหน่วยงานของรัฐที่ให้บริการประชาชนที่ต้องพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติร่วมกับหลักฐานแสดงตน อาทิ บัตรประชาชน หนังสือเดินทาง บัตรสวัสดิการแห่งรัฐ ใบอนุญาตทำงานต่างด้าว บัตรประกันสุขภาพถ้วนหน้า บัตรประกันสังคม บัตรประกันสังคมต่างด้าว ฯลฯ

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตนฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

# คำนำ

การให้บริการประชาชนของภาครัฐหรือภาคเอกชน อาจประกอบด้วยขั้นตอนการพิสูจน์และยืนยันตัวตนซึ่งมีความสำคัญเป็นอย่างยิ่ง รัฐบาลจึงได้ดำเนินงานพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่สอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ และการให้บริการกับประชาชน เพื่อให้เป็นโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้ร่วมกันกำหนดแนวทางการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของประเทศ และจัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ขึ้นประกอบด้วยมาตรฐานทั้งหมดสามฉบับ คือ ขมธอ. 18-2564 [1] ขมธอ. 19-2564 [2] และ ขมธอ. 20-2564 [3] โดยมาตรฐานทั้งสามฉบับดังกล่าวได้ครอบคลุมการใช้ชีวมิติสำหรับสำหรับการพิสูจน์และยืนยันตัวตน

สำหรับข้อเสนอแนะมาตรฐานฉบับนี้ มีจุดมุ่งหมายในการกำหนดมาตรฐานที่เกี่ยวกับการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน ซึ่งเป็นส่วนจำเป็นที่ต่อขยายจากมาตรฐานทั้งสามฉบับข้างต้น เพื่อให้สามารถนำไปปฏิบัติใช้งานได้จริง โดยมีประสิทธิภาพสูงสุด มีความถูกต้องน่าเชื่อถือในระดับสากล มีความโปร่งใส มีความมั่นคงปลอดภัย และรักษาสิทธิส่วนบุคคลของประชาชน รวมทั้งสามารถทำให้แต่ละหน่วยงานทั้งภาครัฐและเอกชนทำงานบูรณาการร่วมกัน โดยสามารถแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างกันได้อย่างมีประสิทธิภาพภายใต้ข้อจำกัดของกฎหมาย

ข้อเสนอแนะมาตรฐานนี้เหมาะกับหน่วยงานภาครัฐหรือภาคเอกชนที่ต้องการนำเทคโนโลยีชีวมิติไปประยุกต์ใช้งานในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งเป็นส่วนหนึ่งของระบบบริหารจัดการอัตลักษณ์บุคคล (Identity Management System: IdMS) โดยข้อเสนอแนะมาตรฐานฉบับนี้ สามารถนำไปประยุกต์ใช้ในหน่วยงานที่เกี่ยวข้องกับการรักษาความปลอดภัยในหน่วยงานราชการ หน่วยงานเอกชน อุตสาหกรรม รวมถึงหน่วยงานของรัฐที่ให้บริการประชาชนที่ต้องพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติร่วมกับหลักฐานแสดงตน เช่น บัตรประชาชน หนังสือเดินทาง บัตรสวัสดิการแห่งรัฐ ใบอนุญาตทำงานต่างด้าว บัตรประกันสุขภาพถ้วนหน้า บัตรประกันสังคม บัตรประกันสังคมต่างด้าว ฯลฯ ทั้งนี้การประยุกต์ใช้ข้อเสนอแนะมาตรฐานนี้ จะเป็นไปในภาพรวมเพื่อประยุกต์ใช้งานเทคโนโลยีชีวมิติให้มีประสิทธิภาพสูงสุดและทำงานได้อย่างเต็มประสิทธิภาพ โดยในกรณีที่มีหน่วยงานกำกับดูแลเฉพาะของแต่ละภาคส่วนกำหนดมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตนเป็นการเฉพาะแล้ว ให้ปฏิบัติตามมาตรฐานของหน่วยงานที่กำกับดูแลเหล่านั้น

# สารบัญ

# สารบัญรูป

หน้า



# สารบัญตาราง

หน้า

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

**เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม ๑: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน**

---

โดยที่เป็นการสมควรกำหนดแนวทางการบริหารจัดการอัตลักษณ์บุคคลเพื่อการพิสูจน์และยืนยันด้วยเทคโนโลยีชีวมิติ เพื่อให้มีการนำเทคโนโลยีชีวมิติไปประยุกต์ใช้กับ การพิสูจน์และยืนยันตัวตนในภาคบริการประชาชนได้อย่างมีประสิทธิภาพสูงสุด มีความน่าเชื่อถือในระดับสากล มีความถูกต้องโปร่งใส มีความปลอดภัย และมีธรรมาภิบาล

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม ๑: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน เลขที่ ขมธอ. ๒๙ เล่ม ๑-๒๕๖๕ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒๑ เมษายน พ.ศ. ๒๕๖๕

ชัยชนะ มิตรพันธ์

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

# ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

# ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 1: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

## 1. ขอบข่าย

ข้อเสนอแนะมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตนฉบับนี้ เป็นข้อเสนอแนะสำหรับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนในประเทศไทย ที่จะต้องประยุกต์ใช้เทคโนโลยีชีวมิติในการพิสูจน์และยืนยันตัวตนสำหรับงานบริการประชาชนในรูปแบบต่าง ๆ ตามหน้าที่และความรับผิดชอบ เพื่อให้มีแนวทางการทำงานร่วมกันในการใช้เทคโนโลยีชีวมิติให้เกิดประสิทธิภาพสูงสุด มีความถูกต้องน่าเชื่อถือในระดับสากล มีความโปร่งใส มีความมั่นคงปลอดภัย และ รักษาสิทธิส่วนบุคคลของประชาชน

ทั้งนี้การประยุกต์ใช้ข้อเสนอแนะมาตรฐานนี้ จะเป็นไปในภาพรวมเพื่อประยุกต์ใช้งานเทคโนโลยีชีวมิติให้มีประสิทธิภาพสูงสุดและทำงานได้อย่างเต็มประสิทธิภาพ โดยในกรณีที่มีหน่วยงานกำกับดูแลเฉพาะของแต่ละภาคส่วนกำหนดมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตนเป็นการเฉพาะแล้ว ให้ปฏิบัติตามมาตรฐานของหน่วยงานที่กำกับดูแลเหล่านั้น

ในข้อเสนอแนะมาตรฐานฉบับนี้ จะใช้รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐานและเนื้อหาเชิงให้ข้อมูล ดังต่อไปนี้

- “ต้อง” ใช้ระบุสิ่งที่เป็นข้อกำหนด ซึ่งต้องปฏิบัติตาม
- “ควร” ใช้ระบุสิ่งที่เป็นข้อแนะนำ
- “อาจ” ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้

## 2. นิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ลักษณะเฉพาะชีวมิติ (biometric characteristic) หมายถึง ลักษณะเฉพาะทางสรีรวิทยาหรือทางพฤติกรรมของแต่ละบุคคล ซึ่งสามารถใช้บอกความแตกต่าง และสามารถสกัดลักษณะเด่นที่สามารถทำซ้ำได้เพื่อใช้ในการรู้จำชีวมิติ [4]

2.2 เอกลักษณ์ (uniqueness) หมายถึง ความเป็นหนึ่งเดียว หรือ ความไม่เหมือนใครของแต่ละบุคคลที่เกิดมาในโลกนี้

2.3 อัตลักษณ์ (identity) หมายถึง คุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้ภายในบริบทที่กำหนด [ขมธอ. 18-2564] [1]

2.4 ตัวระบุอ้างอิงชีวมิติ (biometric reference identifier) หมายถึง ตัวชี้ไปยังระเบียนข้อมูลอ้างอิงชีวมิติในฐานข้อมูลอ้างอิงชีวมิติ [4]

2.5 ลักษณะเฉพาะทางสรีรวิทยา (physiological characteristics) หมายถึง อัตลักษณ์ทางสรีรวิทยาของแต่ละบุคคลซึ่งมีติดตัวมาตั้งแต่เกิด เช่น ลายนิ้วมือ ลายม่านตา ใบหน้า ดีเอ็นเอ

2.6 ลักษณะเฉพาะทางพฤติกรรม (behavioral characteristics) หมายถึง อัตลักษณ์ทางพฤติกรรมของแต่ละบุคคลที่เป็นเอกลักษณ์ เช่น เสียงพูด ลายเซ็น ท่าทางการเดิน

2.7 ระบบบริหารอัตลักษณ์บุคคล (identity management system) หมายถึง ระบบที่ทำหน้าที่บริหารจัดการเกี่ยวกับอัตลักษณ์บุคคล [5]

2.8 ระบบรู้จำชีวมิติอัตโนมัติ (automated biometric recognition system) หมายถึง ระบบที่ใช้ทำหน้าที่ในการรู้จำชีวมิติโดยอัตโนมัติ โดยใช้ในการพิสูจน์ยืนยันตัวตน (personal verification) หรือการระบุตัวตน (personal identification) ด้วยลักษณะเฉพาะชีวมิติ

2.9 คะแนนความเหมือน (similarity score) หมายถึง คะแนนเปรียบเทียบระหว่างข้อมูลตัวอย่างชีวมิติกับข้อมูลอ้างอิงชีวมิติที่อยู่ในฐานข้อมูลว่ามีความเหมือนกันอยู่เพียงใด โดยถ้าค่าคะแนนความเหมือนมากจะหมายความว่า มีความเหมือนกันมากระหว่างสองข้อมูลชีวมิติ

2.10 การพิสูจน์ยืนยันชีวมิติ (biometric verification) หมายถึง กระบวนการในการพิสูจน์ยืนยันชีวมิติของผู้กล่าวอ้างผ่านการเปรียบเทียบชีวมิติอ้างอิง [4]

2.11 การระบุชีวมิติ (biometric identification) หมายถึง กระบวนการค้นหาชีวมิติในฐานข้อมูลที่ลงทะเบียนไว้ก่อน โดยตอบกลับเป็นตัวระบุอัตลักษณ์อ้างอิงชีวมิติซึ่งบ่งชี้ไปถึงแต่ละบุคคล [4]

2.12 เทคโนโลยีผ่านการพัฒนา (mature technology) หมายถึง เทคโนโลยีที่ได้ทำการพัฒนามาเป็นระยะเวลาหนึ่งแล้ว ได้มีการใช้งานจริง มีผลิตภัณฑ์สู่การใช้งานในวงกว้าง มีการปรับปรุงแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นขณะใช้งานจริง

2.13 ชีวมิติหลายประเภท (multi-model biometric) หมายถึง การใช้งานชีวมิติแบบผสมผสาน โดยใช้งานชีวมิติมากกว่าหนึ่งประเภทในการทำงานพิสูจน์ยืนยันตัวตน หรือระบุตัวตน เช่น การใช้ใบหน้าร่วมกับม่านตาในระบบการพิสูจน์ยืนยันตัวตน

2.14 อัตราการเข้าคู่ผิดพลาด (false match rate: FMR) หมายถึง อัตราความผิดพลาดที่ระบบเข้าคู่ระหว่างข้อมูลตัวอย่างชีวมิติกับข้อมูลอ้างอิงชีวมิติในฐานข้อมูล โดยระบบเข้าคู่บุคคลคนละคนกันและให้คะแนนความเหมือนที่มีความคล้ายกัน

2.15 อัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) หมายถึง อัตราความผิดพลาดที่ระบบไม่เข้าคู่ให้ถูกต้องระหว่างข้อมูลตัวอย่างชีวมิติกับข้อมูลอ้างอิงชีวมิติในฐานข้อมูล โดยระบบไม่เข้าคู่บุคคลคนเดียวกันและให้คะแนนความเหมือนที่แตกต่างกัน

2.16 ลักษณะสำคัญชีวมิติ (biometric feature) หมายถึง ตัวเลขหรือสัญลักษณ์ที่สกัดจากข้อมูลตัวอย่างชีวมิติและใช้ในการเปรียบเทียบ [4]

2.17 ข้อมูลตัวอย่างชีวมิติ (biometric sample) หมายถึง ลักษณะเฉพาะชีวมิติที่แทนด้วยข้อมูลแอนะล็อกหรือดิจิทัลก่อนการสกัดลักษณะสำคัญชีวมิติ [4] เช่น ภาพใบหน้า ภาพลายนิ้วมือ ภาพม่านตา สัญญาณเสียงพูด

2.18 ข้อมูลอ้างอิงชีวมิติ (biometric reference) หมายถึง ข้อมูลตัวอย่างชีวมิติอย่างน้อยหนึ่งข้อมูล ซึ่งอาจมี

มากกว่าหนึ่งก็ได้ โดยเป็นลักษณะประจำของบุคคลเจ้าของข้อมูลชีวมิติและถูกใช้เป็นตัวเปรียบเทียบชีวมิติ [4]

2.19 ข้อมูลชีวมิติ (biometric data) หมายถึง ข้อมูลตัวอย่างชีวมิติ หรือ การรวบรวมข้อมูลตัวอย่างชีวมิติ ที่อยู่ในทุกกระบวนการ [4]

2.20 เทมเพลตชีวมิติ (biometric template) หมายถึง ชุดข้อมูลลักษณะสำคัญชีวมิติที่เก็บไว้ สามารถนำไปเปรียบเทียบกับลักษณะสำคัญที่สกัดได้จากข้อมูลตัวอย่างชีวมิติที่ได้จากบุคคลกล่าวอ้าง [4]

2.21 คุณภาพข้อมูลตัวอย่างชีวมิติ (biometric sample quality) หมายถึง ค่าที่สะท้อนถึงคุณภาพของข้อมูลตัวอย่างชีวมิติ

2.22 การประเมินคุณภาพข้อมูลตัวอย่างชีวมิติ (biometric sample quality assessment) หมายถึง ขั้นตอนวิธีในการประเมินค่าคุณภาพของข้อมูลตัวอย่างชีวมิติ

2.23 การโจมตีหลอกระบบ (presentation attack) หมายถึง บุคคลนำเสนอลักษณะเฉพาะชีวมิติปลอมเพื่อหลอกระบบรู้จำชีวมิติอัตโนมัติ

2.24 เครื่องมือโจมตีหลอกระบบ (presentation attack instrument: PAI) หมายถึง อุปกรณ์ปลอมแปลงเพื่อแอบอ้างเป็นเจ้าของลักษณะเฉพาะชีวมิติ หรือปลอมแปลงเพื่อหลบหลีกการตรวจสอบลักษณะเฉพาะชีวมิติ

2.25 การตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) หมายถึง กระบวนการที่ใช้ตรวจสอบการปลอมแปลงลักษณะเฉพาะชีวมิติของบุคคลที่เข้ามาใช้งานระบบ

2.26 รูปแบบการแลกเปลี่ยนชีวมิติร่วมกัน (common biometric exchange formats: CBEF) หมายถึง ข้อมูลชีวมิติที่เก็บด้วยรูปแบบโครงสร้างข้อมูลตามมาตรฐานที่กำหนด ซึ่งพร้อมในการแลกเปลี่ยนข้อมูล

## 3. อักษรย่อ

อักษรย่อที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

| อักษรย่อ | คำเต็ม | คำภาษาไทย |
|---|---|---|
| CBEF | Common Biometric Exchange Formats | รูปแบบการแลกเปลี่ยนชีวมิติร่วมกัน |
| DET | Detection-Error Tradeoff | กราฟเส้นโค้งการแลกเปลี่ยนการตรวจจับที่ผิดพลาด |
| FMR | False Match Rate | อัตราการเข้าคู่ผิดพลาด |
| FNMR | False Non-Match Rate | อัตราการไม่เข้าคู่ผิดพลาด |
| IdM | Identity Management | การบริหารอัตลักษณ์บุคคล |
| IdMS | Identity Management System | ระบบบริหารอัตลักษณ์บุคคล |
| NIST | National Institute of Standards and Technology | สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ โดยกระทรวงพาณิชย์ของสหรัฐอเมริกา |
| PA | Presentation Attack | การโจมตีหลอกระบบ |
| PAD | Presentation Attack Detection | การตรวจจับการโจมตีหลอกระบบ |
| PAI | Presentation Attack Instrument | เครื่องมือโจมตีหลอกระบบ |
| PAP | Presentation Attack Protection | การป้องกันการโจมตีหลอกระบบ |

## 4. ภาพรวมการใช้งานเทคโนโลยีชีวมิติกับระบบบริหารอัตลักษณ์บุคคล (IdMS)

บุคคล หรือ มนุษย์ทุกคนในโลกนี้ ตั้งแต่เกิดมาทุกคนมีเอกลักษณ์ (uniqueness) หรือความเป็นหนึ่งเดียวที่ไม่เหมือนใครในโลก ซึ่งเอกลักษณ์นี้สามารถพิสูจน์ได้จากอัตลักษณ์ (identity) ซึ่งเป็นคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้ [1]

ลักษณะเฉพาะชีวมิติ (biometric characteristics) ถูกกำหนดให้เป็นอัตลักษณ์อีกอย่างหนึ่งและเป็นสิ่งที่ใช้ยืนยันตัวตน (authenticator) ได้ [1] โดยแบ่งเป็น ลักษณะเฉพาะทางสรีรวิทยา (physiological characteristics) เช่น ลายนิ้วมือ ลายม่านตา ใบหน้า ลายเส้นเลือด ดีเอ็นเอ และ ลักษณะเฉพาะทางพฤติกรรม (behavioral characteristics) เช่น เสียง ลายเซ็น รูปแบบการเดิน

ระบบบริหารอัตลักษณ์บุคคล (identity management system: IdMS) [5] เป็นระบบที่ใช้บริหารจัดการเกี่ยวกับอัตลักษณ์ของบุคคล จะต้องมีเครื่องมือในการพิสูจน์ยืนยันตัวบุคคลและระบุตัวบุคคล และหนึ่งในเครื่องมือหลักคือ ระบบรู้จำชีวมิติอัตโนมัติ (automated biometric recognition system) ซึ่งสามารถแยกแยะแต่ละบุคคลออกจากกันได้ด้วยลักษณะเฉพาะชีวมิติ ซึ่งอาจมีลักษณะเฉพาะชีวมิติอย่างน้อยหนึ่งประเภท หรืออาจใช้ลักษณะเฉพาะชีวมิติหลายประเภท (multi-model biometric) ประกอบกัน เช่น ใบหน้า ลายนิ้วมือ ลายม่านตา โดยลักษณะเฉพาะชีวมิติจะต้องมีเพียงพอที่ใช้ในการแยกความแตกต่างของบุคคลเป้าหมายออกจากบุคคลอื่น ๆ ภายใต้ระบบบริหารอัตลักษณ์บุคคลนั้น ซึ่งจะนำไปสู่การพิสูจน์ยืนยันความเป็นเอกลักษณ์ของแต่ละบุคคลได้

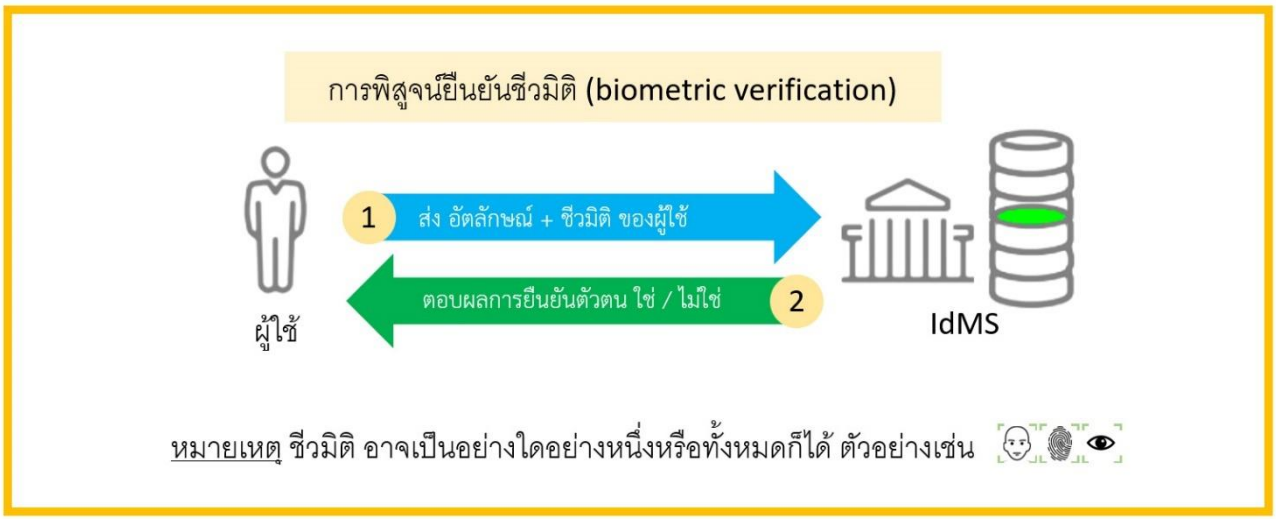
หมายเหตุ: มาตรฐานเล่มนี้ ไม่ได้เกี่ยวข้องกับการกำหนดกรอบการทำงานของระบบบริหารอัตลักษณ์บุคคล (IdMS) ซึ่งจะมีรายละเอียดอยู่ในมาตรฐาน ISO/IEC 24760-1:2011 [5] แต่ข้อกำหนดมาตรฐานเล่มนี้เป็นแนวทางในการใช้งานชีวมิติในการบริหารอัตลักษณ์บุคคล โดยมีแนวทางเริ่มต้นจากมาตรฐาน ISO/IEC TR 29144:2014 [6]

เมื่อประยุกต์ใช้ลักษณะเฉพาะชีวมิติกับระบบบริหารอัตลักษณ์บุคคล หรือ IdMS แล้ว ลักษณะเฉพาะชีวมิติจะเป็นเพียงสิ่งที่ให้ความมั่นใจในการยืนยันตัวบุคคล ว่าบุคคลนี้ เป็นบุคคลคนเดียวกับที่ลงทะเบียนลักษณะเฉพาะชีวมิติไว้กับระบบ IdMS ไว้ก่อนหน้าหรือไม่ ดังนั้น ลักษณะเฉพาะชีวมิติสามารถใช้ได้เพียงการยืนยันบุคคลที่มีชุดข้อมูลชีวมิติที่ลงทะเบียนอยู่ก่อนหน้าเท่านั้น [6]

กระบวนการใช้งานชีวมิติใน IdMS เกี่ยวข้องกับงานบริการประชาชนและงานนิติวิทยาศาสตร์ ในมาตรฐานเล่มนี้จะเน้นการใช้งานบริการประชาชนเป็นหลัก การใช้งานชีวมิติในระบบบริหารจัดการอัตลักษณ์โดยทั่วไปแล้วมีสองประเภท คือการพิสูจน์ยืนยันชีวมิติ และการระบุชีวมิติโดยมีรายละเอียด ดังต่อไปนี้

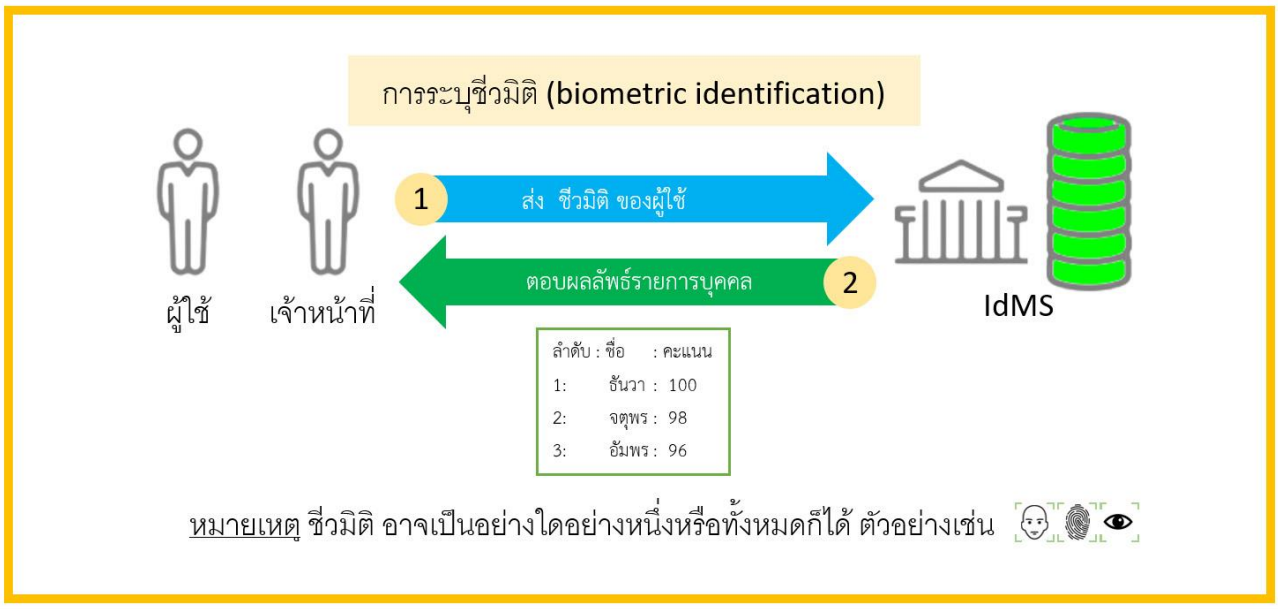
**(1) การพิสูจน์ยืนยันชีวมิติ (biometric verification)** หมายถึง กระบวนการพิสูจน์ยืนยันชีวมิติของผู้ใช้หรือผู้กล่าวอ้างเป็นเจ้าของอัตลักษณ์ โดยเมื่อบุคคลเรียกร้องหรือกล่าวอ้างการเป็นเจ้าของหลักฐานแสดงตนนั้น ๆ เช่น บัตรประชาชน หนังสือเดินทาง หรือ ใบอนุญาตทำงานต่างด้าว IdMS จะตอบสนองการเรียกร้อง ซึ่งโดยปกติแล้วจะเป็นระบบอัตโนมัติ ซึ่งจะมีกระบวนการเปรียบเทียบข้อมูลตัวอย่างชีวมิติของผู้เรียกร้อง กับข้อมูลอ้างอิงชีวมิติที่เชื่อมโยงกับข้อมูลอัตลักษณ์ (เช่น เลขประจำตัวประชาชน) ซึ่งได้ลงทะเบียนเก็บไว้ก่อนล่วงหน้าในฐานข้อมูลของ IdMS โดยการเปรียบเทียบข้อมูลชีวมิติจะเป็นลักษณะหนึ่งต่อหนึ่ง (one-to-one) ผลของการเปรียบเทียบข้อมูลชีวมิติจะอยู่ในรูปคะแนนความเหมือน (similarity score) ระหว่างบุคคลผู้กล่าวอ้างกับบุคคลซึ่งอยู่ในฐานข้อมูล ค่าคะแนนความเหมือนนี้จะถูกตัดสินโดยค่าเทรชโฮลด์ (threshold) ซึ่งเป็นค่าคะแนนความเชื่อมั่นที่ยอมรับได้ ที่ถูกตั้งไว้อย่างเหมาะสมตามข้อกำหนดก่อนล่วงหน้า ถ้าค่าคะแนนความเหมือนสูงกว่าหรือเท่ากับค่าเทรชโฮลด์ ระบบจะตอบ “ใช่” แต่ถ้าค่าคะแนนความเหมือนต่ำว่าค่าเทรชโฮลด์ ระบบจะตอบ “ไม่ใช่” ซึ่งโดยปกติแล้วระบบรู้จำ

ชีวมิติอัตโนมัติจะให้ผลตอบสนองอย่างรวดเร็ว ดังแสดงในรูปที่ 1




**รูปที่ 1 การพิสูจน์ยืนยันชีวมิติ (biometric verification)**

**(2) การระบุชีวมิติ (biometric identification)** หมายถึง กระบวนการค้นหาระบุตัวบุคคลด้วยชีวมิติของบุคคลที่มีข้อมูลชีวมิติอยู่ในฐานข้อมูล IdMS โดยเมื่อสามารถเก็บข้อมูลตัวอย่างชีวมิติของผู้ใช้หรือบุคคลเป้าหมายได้ เจ้าหน้าที่จะส่งข้อมูลตัวอย่างชีวมิติเข้าไปค้นหาระบุตัวบุคคลในระบบ IdMS โดยกระบวนการจะเปรียบเทียบข้อมูลตัวอย่างชีวมิติของบุคคลเป้าหมายกับข้อมูลอ้างอิงชีวมิติของทุก ๆ บุคคลที่มีอยู่ในฐานข้อมูลของ IdMS ซึ่งได้ลงทะเบียนเก็บข้อมูลตัวอย่างชีวมิติไว้ก่อนล่วงหน้า ซึ่งการเปรียบเทียบจะเป็นลักษณะหนึ่งต่อกลุ่ม (one-to-many) ผลของการระบุตัวบุคคลอาจจะเป็นบุคคลที่มีค่าคะแนนความเหมือนสูงที่สุด หรือจะอยู่ในรูปแบบรายการบุคคลที่มีชีวมิติที่มีค่าคะแนนความเหมือนใกล้เคียงกับบุคคลเป้าหมาย โดยเรียงลำดับของบุคคลตามคะแนนความเหมือน จากบุคคลที่มีคะแนนความเหมือนมากที่สุด ตามด้วยบุคคลที่มีคะแนนความเหมือนที่ลดต่ำลงไป โดยจำนวนบุคคลในรายการแสดงจะถูกกำหนดโดยเจ้าหน้าที่ที่ใช้งาน เช่น 10 บุคคลแรกที่มีคะแนนความเหมือนสูงสุดเมื่อเปรียบเทียบกับบุคคลเป้าหมาย โดยปกติแล้ว IdMS ที่ทำงานในส่วนนี้จะให้ผลตอบสนองภายในระยะเวลาจำกัดช่วงหนึ่งซึ่งอาจไม่ทันที โดยเวลาตอบสนองจะแปรผันตามจำนวนข้อมูลอ้างอิงชีวมิติในฐานข้อมูล IdMS ที่เก็บไว้ก่อนหน้าและสมรรถนะของระบบที่ใช้ในการคำนวณเปรียบเทียบชีวมิติ ดังแสดงในรูปที่ 2




**รูปที่ 2 การระบุชีวมิติ (biometric identification)**

ตารางที่ 1 แสดงการเปรียบเทียบรูปแบบการใช้งานชีวมิติทั้งสองประเภท ซึ่งได้ทำการเปรียบเทียบข้อมูลนำเข้า ผลลัพธ์ที่ได้ และเวลาในการตอบสนองผลลัพธ์

**ตารางที่ 1 การเปรียบเทียบกระบวนการใช้งานชีวมิติสำหรับ IdMS**

| ประเภทการใช้งาน | ข้อมูลนำเข้า | ผลลัพธ์ | เวลาในการตอบสนองผลลัพธ์ |
|---|---|---|---|
| **การพิสูจน์ยืนยันชีวมิติ** | อัตลักษณ์ + ชีวมิติ (ชีวมิติอย่างน้อยหนึ่งประเภท) | ใช่ / ไม่ใช่ | เนื่องจากเป็นการเปรียบเทียบหนึ่งต่อหนึ่งโดยใช้ระบบรู้จำชีวมิติอัตโนมัติ ระบบควรตอบสนองทันที |
| **การระบุชีวมิติ** | ชีวมิติ (ถ้ามีหลายประเภทจะช่วยให้ระบุตัวตนให้แม่นยำยิ่งขึ้น) | รายการบุคคลตามลำดับความเหมือน | เนื่องจากเป็นการเปรียบเทียบหนึ่งต่อกลุ่ม ขึ้นกับจำนวนบุคคลในฐานข้อมูลและสมรรถนะของระบบ ระบบควรตอบสนองในกรอบเวลาที่กำหนด เช่น ภายใน 24 ชั่วโมง |

การนำรูปแบบทั้งสองไปประยุกต์ใช้งาน ขึ้นอยู่กับวัตถุประสงค์และลักษณะงานของแต่ละหน่วยงาน ซึ่งอาจมีการใช้งานได้หลายรูปแบบในหน่วยงานเดียวกัน เช่น หน่วยงานทั่วไปที่มีวัตถุประสงค์ในการใช้ชีวมิติในการยืนยันตัวตน ไม่ได้ใช้เพียงประเภทการพิสูจน์ยืนยันชีวมิติเท่านั้น แต่อาจใช้ประเภทการระบุชีวมิติในการลงทะเบียนเพื่อป้องกันไม่ให้หนึ่งบุคคลมีระเบียนที่ซ้ำซ้อน เช่น ในกรณีของบัตรประจำตัวประชาชน ซึ่งโดยปกติแล้วบุคคลควรมีเลขประจำตัวประชาชนเพียงหมายเลขเดียวเท่านั้น ยกเว้นในกรณีที่บุคคลอยู่ภายใต้โครงการคุ้มครองพยาน ซึ่งอาจมีเลขประจำตัวประชาชนอีกเลขหนึ่ง หรือในกรณีของหนังสือเดินทาง โดยปกติแล้วในเวลาใดเวลาหนึ่ง บุคคลควรมีหนังสือเดินทางได้เพียงฉบับเดียวเท่านั้น ยกเว้นในกรณีที่บุคคลทำงานให้หน่วยงานราชการ ซึ่งอาจมีหนังสือเดินทางราชการอีกหนึ่งฉบับซึ่งใช้ในกรณีการเดินทางไปราชการ

สำหรับลำดับของหัวข้อต่าง ๆ เกี่ยวกับข้อเสนอแนะมาตรฐานเกี่ยวกับการใช้งานเทคโนโลยีชีวมิติกับระบบบริหารอัตลักษณ์บุคคลเพื่องานบริการประชาชน มีทั้งหมด 5 หัวข้อ โดยเรียงลำดับดังต่อไปนี้

- หัวข้อที่ 5 ข้อควรพิจารณาก่อนการนำเทคโนโลยีชีวมิติไปใช้งานกับระบบบริหารอัตลักษณ์บุคคล ซึ่งกล่าวถึง ข้อควรพิจารณาในการเลือกประเภทลักษณะเฉพาะชีวมิติ ข้อควรพิจารณาในการเลือกระบบรู้จำชีวมิติอัตโนมัติ ข้อควรระวังเกี่ยวกับการเก็บและบันทึกข้อมูลชีวมิติ ข้อควรพิจารณาในการกำหนดบทบาทของบุคลากรสำหรับทำงานร่วมกับระบบรู้จำชีวมิติอัตโนมัติ และข้อเสนอแนะในการสร้างความเชื่อมั่นในการรวมกันของฐานข้อมูล
- หัวข้อที่ 6 ข้อเสนอแนะเกี่ยวกับการใช้เทคโนโลยีชีวมิติสำหรับการบริหารอัตลักษณ์บุคคล ซึ่งเป็นหัวใจของข้อเสนอแนะมาตรฐานเล่มนี้ ในหัวข้อนี้จะเกี่ยวข้องกับ ข้อเสนอแนะภาพรวมการเก็บข้อมูลชีวมิติ มาตรฐานการบันทึกข้อมูลชีวมิติ ข้อเสนอแนะการประเมินคุณภาพข้อมูลอ้างอิงชีวมิติ มาตรฐานการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน แนวทางการจัดการข้อมูลชีวมิติและข้อมูลอื่น และข้อยกเว้นอื่น ๆ
- หัวข้อที่ 7 ข้อเสนอแนะเกี่ยวกับการรักษาความปลอดภัยข้อมูลชีวมิติกับระบบบริหารอัตลักษณ์บุคคล ในหัวข้อนี้กล่าวถึงการรักษาความปลอดภัยข้อมูลชีวมิติ ซึ่งแบ่งเป็นสองส่วน คือ ส่วนการป้องกันการโจมตีหลอก และส่วนการป้องกันเทมเพลตชีวมิติ
- หัวข้อที่ 8 ข้อเสนอแนะเกี่ยวกับสิทธิส่วนบุคคลกับข้อมูลชีวมิติ กล่าวถึงประเด็นต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและข้อมูลชีวมิติ
- หัวข้อที่ 9 ข้อเสนอแนะการประยุกต์ใช้งานมาตรฐานเพื่อการพิสูจน์ยืนยันตัวตน กล่าวถึงตัวอย่างการนำข้อเสนอแนะมาตรฐานไปประยุกต์ใช้งานกับระบบรู้จำชีวมิติอัตโนมัติในการลงทะเบียน การพิสูจน์ยืนยันตัวตน และการระบุตัวตน

## 5. ข้อควรพิจารณาก่อนการนำเทคโนโลยีชีวมิติไปใช้งานกับระบบบริหารอัตลักษณ์บุคคล

ก่อนที่จะนำเทคโนโลยีชีวมิติไปประยุกต์ใช้งานกับระบบบริหารอัตลักษณ์บุคคล IdMS ควรพิจารณาประโยชน์ที่ได้รับจากการนำไปใช้งาน พิจารณาข้อดี ข้อเสีย ข้อควรระวัง ความปลอดภัยของการใช้งาน รวมไปถึงเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและสิทธิส่วนบุคคล โดยข้อควรพิจารณาก่อนการนำเทคโนโลยีชีวมิติไปใช้งานใน IdMS สามารถแบ่งได้เป็น 5 หัวข้อสำคัญดังต่อไปนี้

(1) ข้อควรพิจารณาในการเลือกประเภทลักษณะเฉพาะชีวมิติ

(2) ข้อควรพิจารณาในการเลือกระบบรู้จำชีวมิติอัตโนมัติ

(3) ข้อควรระวังเกี่ยวกับการเก็บและการบันทึกข้อมูลชีวมิติ

(4) ข้อควรพิจารณาในการกำหนดบทบาทของบุคลากรกับระบบรู้จำชีวมิติอัตโนมัติ

(5) ข้อเสนอแนะในการสร้างความเชื่อมั่นในการรวมกันของฐานข้อมูล

โดยมีรายละเอียดของแต่ละหัวข้อ ดังต่อไปนี้

### 5.1 ข้อควรพิจารณาในการเลือกประเภทลักษณะเฉพาะชีวมิติ

เนื่องจากลักษณะเฉพาะชีวมิติมีหลายประเภทและมีข้อดีข้อเสียที่แตกต่างกันไป โดยรายละเอียดมีอธิบายในสมุดปกขาว เรื่อง “การพิสูจน์และยืนยันตัวตนด้วยระบบไบโอเมตริก” [7] ดังนั้นหน่วยงานที่ต้องการประยุกต์ใช้เทคโนโลยีชีวมิติหรือผู้ให้บริการควรเลือกใช้งานประเภทลักษณะเฉพาะชีวมิติตามความเหมาะสม การเลือกลักษณะเฉพาะชีวมิติที่จะใช้งานในระบบบริหารอัตลักษณ์บุคคล IdMS จะต้องประเมินความเหมาะสมอย่างละเอียดว่า ลักษณะเฉพาะชีวมิติประเภทที่จะเลือกใช้นั้น มีเหมาะสมกับงานที่ต้องการประยุกต์ใช้และตอบโจทย์ปัญหาที่ต้องการนำเทคโนโลยีชีวมิติมาช่วยแก้ไขปัญหาได้อย่างชัดเจน โดยมีหลักในการพิจารณาเลือกประเภทของลักษณะเฉพาะชีวมิติที่เหมาะสมสำหรับการใช้งานบริการประชาชนดังต่อไปนี้

**(1) เทคโนโลยีที่ผ่านการพัฒนา (mature technology)** ผู้ให้บริการควรพิจารณาเลือกเทคโนโลยีชีวมิติที่มีการพัฒนาและใช้งานมาเป็นระยะเวลานานพอที่จะแก้ไขปัญหาต่าง ๆ ส่วนใหญ่ที่เกิดขึ้นแล้วในอดีต ลักษณะเฉพาะชีวมิติที่มีเทคโนโลยีที่ผ่านการพัฒนาแล้ว ได้แก่ ลายนิ้วมือ ลายม่านตา ใบหน้า ลักษณะเฉพาะชีวมิติที่ยังอยู่ในช่วงพัฒนา ได้แก่ ลายเส้นเลือด ดีเอ็นเอ

**(2) ความสามารถในการใช้งาน (usability)** ผู้ให้บริการควรพิจารณาลักษณะเฉพาะชีวมิติประเภทที่ให้ความสะดวกในการใช้งานเป็นส่วนสำคัญในงานบริการประชาชน รวมถึงพิจารณาการยอมรับของผู้ใช้กับการใช้ลักษณะเฉพาะชีวมิติแต่ละประเภท ผู้คนโดยทั่วไปสามารถเข้าถึงเซนเซอร์ชีวมิติได้อย่างสะดวกจะส่งผลให้ระบบมีประสิทธิผลที่ดี ในกรณีที่ผู้ใช้งานเป็นวงกว้าง ต้องพิจารณาข้อจำกัดที่เกิดขึ้นจาก

(2.1) ความพิการ ทำให้ไม่สามารถเก็บข้อมูลตัวอย่างชีวมิติได้ โดยพิการขาดอวัยวะที่ใช้เป็นลักษณะเฉพาะชีวมิติ หรือลักษณะเฉพาะชีวมิติผิดรูปไม่สามารถเก็บได้ เช่น แขนขาด มือขาด หรือนิ้วขาด หรือ อุบัติเหตุหรือไฟไหม้ทำให้ใบหน้าผิดรูป ไม่สามารถเก็บภาพใบหน้าเพื่อใช้กับระบบรู้จำใบหน้าได้

(2.2) อาชีพ ที่ใช้อวัยวะส่วนที่เกี่ยวข้องกับลักษณะเฉพาะชีวมิติทำงาน จนลักษณะเฉพาะชีวมิติมีการเปลี่ยนสภาพไม่สามารถเก็บข้อมูลได้ เช่น ลายนิ้วมือของ ช่างก่อสร้าง ชาวประมง เจ้าหน้าที่ธนาคารที่นับธนบัตรด้วยมือ หรือลูกจ้างอุตสาหกรรมการเกษตรที่ใช้มือทำงาน สภาพผิวหนังที่เสื่อมจากการทำงาน ทำให้ไม่สามารถเก็บข้อมูลลายนิ้วมืออย่างสมบูรณ์หรือมีคุณภาพที่ดีได้

(2.3) สุขภาพ ที่ไม่ปกติทำให้ไม่สามารถเก็บข้อมูลชีวมิติได้ เช่น ไม่สามารถเก็บลายนิ้วมือกับผู้ที่มีผิวหนังลอก และผู้เป็นโรคทางกรรมพันธุ์เช่น Adermatoglyphia ที่ไม่มีลายนิ้วมือ หรือ ลายม่านตาสามารถเปลี่ยนแปลงได้จากการเป็นโรคบางชนิดหรือการใช้ยาบางชนิดได้ หรือ ใบหน้าที่มีการเปลี่ยนแปลงเนื่องจากสุขภาพไม่ปกติ เช่น การรักษาโรคมะเร็งด้วยการฉายแสง อาจมีการเปลี่ยนแปลงทำให้ไม่สามารถเปรียบเทียบกับใบหน้าปกติได้

**(3) ความเป็นเอกลักษณ์ (uniqueness)** ผู้ให้บริการควรพิจารณาลักษณะเฉพาะชีวมิติที่สามารถใช้พิสูจน์และยืนยันตัวตนได้ ฝาแฝดไข่ใบเดียวกันจะมีใบหน้าและดีเอ็นเอที่เหมือนกัน รวมไปถึงเครือญาติที่มีความใกล้ชิดทางพันธุกรรมจะมีใบหน้าที่คล้ายคลึงกัน ทำให้เกิดปัญหากับระบบรู้จำใบหน้า ในทางตรงกันข้าม ลายนิ้วมือและลายม่านตามีความเป็นเอกลักษณ์ แม้แต่ฝาแฝดไข่ใบเดียวกันที่มีดีเอ็นเอเหมือนกันก็มีลายนิ้วมือและลายม่านตาที่แตกต่างกัน นอกจากนี้ลักษณะเฉพาะชีวมิติแต่ละประเภทมีความแม่นยำแตกต่างกันไปดังต่อไปนี้

(3.1) ลายม่านตามีความเป็นเอกลักษณ์สูงสุดในลักษณะเฉพาะชีวมิติ มนุษย์ปกติจะมีม่านตาสองข้างทำให้สามารถระบุตัวบุคคลได้อย่างแม่นยำสูงมาก ตามธรรมชาติแล้วลายม่านตาจะให้ความแม่นยำในการรู้จำสูงสุดเมื่อเปรียบเทียบกับลักษณะเฉพาะชีวมิติแบบอื่น ๆ นั่นหมายถึงการยืนยันตัวตนผิดพลาดแทบเป็นไปไม่ได้ แต่ลายม่านตามีความผิดพลาดในการปฏิเสธการยืนยันตัวตนที่สูงกว่าลักษณะเฉพาะชีวมิติอื่น ๆ เนื่องจากการเก็บข้อมูลลายม่านตามีอุปสรรคมาก เช่น การเก็บข้อมูลลายม่านตาต้องมีการควบคุมสภาพแวดล้อมของแสงและระยะห่าง การบดบังของเปลือกตา ขนตา แว่นตา และคอนแทคเลนส์

(3.2) ลายนิ้วมือให้ความแม่นยำรองจากลายม่านตา และมีความเป็นเอกลักษณ์สูงมากถ้าใช้ทั้งสิบนิ้ว ทำให้โอกาศผิดพลาดในการยืนยันตัวตนเกิดขึ้นได้ยากมาก ความผิดพลาดในการปฏิเสธการยืนยันตัวตนน้อยกว่าลายม่านตาเนื่องจากสภาพแวดล้อมและเซนเซอร์ในการเก็บภาพลายนิ้วมือส่วนใหญ่อยู่ในสภาพแวดล้อมที่ถูกควบคุม นอกจากนี้เทคโนโลยีการรู้จำลายนิ้วมือได้ถูกพัฒนามาเป็นเวลานาน รวมทั้งมีเทคโนโลยีที่ใช้ในการแก้ปัญหาที่เกิดขึ้นอย่างหลากหลาย

(3.3) ใบหน้าให้ความแม่นยำที่ต่ำที่สุดเมื่อเปรียบเทียบกับลักษณะเฉพาะชีวมิติสองประเภทแรก เนื่องจากมนุษย์มีเพียงใบหน้าเดียว และมีการเปลี่ยนแปลงต่อเนื่องตามอายุที่เพิ่มขึ้น นอกจากนี้ลักษณะใบหน้ามีความเกี่ยวข้องกับพันธุกรรม ฝาแฝดไข่ใบเดียวกันจะมีใบหน้าที่เหมือนกัน หรือในกรณีที่มีความสัมพันธ์ทางพันธุกรรมเช่น พ่อหรือแม่กับลูก นอกจากนี้ใบหน้ายังเกิดการเปลี่ยนแปลงเมื่อเวลาเปลี่ยนไป การผ่าตัดใบหน้าอาจทำให้ใบหน้าแตกต่างจากเดิมและไปเหมือนกับบุคคลอื่นได้

**(4) ความคงทนถาวร (permanence)** ข้อมูลชีวมิติของแต่ละบุคคลสามารถเปลี่ยนแปลงได้เมื่อเวลาเปลี่ยนไปตามธรรมชาติ และลักษณะเฉพาะชีวมิติแต่ละประเภทมีการเปลี่ยนแปลงไม่เท่ากัน ควรพิจารณาลักษณะเฉพาะชีวมิติประเภทที่ให้ความคงทนไม่เปลี่ยนแปลงไปในระยะเวลาที่ต้องการใช้งาน

และให้มีผลกระทบน้อยที่สุดต่อความสามารถของระบบในการยืนยันและระบุตัวตนได้อย่างถูกต้องแม่นยำ ซึ่งลักษณะเฉพาะชีวมิติแต่ละประเภทมีการเปลี่ยนแปลงไปตามเวลา ดังต่อไปนี้

(4.1) ลายนิ้วมือแม้ว่ารูปแบบจะไม่เปลี่ยนแปลงเนื่องจากพัฒนาตั้งแต่อยู่ในครรภ์มารดา แต่มีการเปลี่ยนขนาดของเส้นสันและระยะห่างตั้งแต่แรกเกิดจนเข้าสู่วัยรุ่น [8] จากนั้นจะมีการเปลี่ยนแปลงรูปแบบตามเวลาน้อยมากเมื่อบุคคลโตเต็มวัย แต่คุณภาพของลายนิ้วมือจะมีคุณภาพต่ำลงเนื่องจากความแห้งหรือมีรอยแยกเมื่อมีอายุมากขึ้นหรือเข้าสู่วัยชรา การเปลี่ยนแปลงของลายนิ้วมือเกิดขึ้นได้ในกรณีอุบัติเหตุที่เกี่ยวข้องกับบริเวณลายนิ้วมือ ความเจ็บป่วยบางชนิด หรือการจงใจทำลายหรือเปลี่ยนแปลงลายนิ้วมือของเจ้าของลายนิ้วมือเอง

(4.2) ลายม่านตาจะไม่เปลี่ยนแปลงในช่วงระยะเวลาจำกัด ลายม่านตาของเด็กจะมีความเสถียรตั้งแต่อายุ 8 ขวบ [8] แต่ยังไม่มีงานวิจัยที่สนับสนุนความคงทนถาวรของลายม่านตาในช่วงอายุคนจนถึงวัยชรา เนื่องจากไม่มีฐานข้อมูลที่มีการเก็บข้อมูลลายม่านตาในช่วงเวลาต่าง ๆ ที่ยาวนานของอายุคนจำนวนมากมาสนับสนุนความคงทนไม่เปลี่ยนแปลงเหมือนกับลายนิ้วมือ การเปลี่ยนแปลงของลายม่านตาเกิดขึ้นได้ในกรณีอุบัติเหตุ และ ความเจ็บป่วยด้วยโรคที่เกี่ยวข้องกับดวงตา

(4.3) ใบหน้ามีโอกาสเปลี่ยนแปลงมากที่สุดเมื่อเทียบกับลายนิ้วมือและลายม่านตา ใบหน้าเปลี่ยนแปลงตั้งแต่แรกเกิดจนถึงวัยชรา ไม่ควรใช้ระบบรู้จำใบหน้ากับเด็กตั้งแต่แรกเกิดจนถึง 5 ขวบเนื่องจากไม่เสถียร ใบหน้าจะเสถียรเมื่อเด็กมีอายุมากกว่า 13 ปี [8] จากนั้นถ้ามีระยะเวลาในการเก็บภาพใบหน้าห่างกันเกิน 6 ปี ระบบรู้จำใบหน้าจะเริ่มมีปัญหาโดยความแม่นยำในการรู้จำใบหน้าจะตกต่ำลงอย่างมีนัยยะสำคัญโดยอ้างอิงจาก [9] ดังนั้นถ้าจะใช้งานลักษณะเฉพาะชีวมิติประเภทใบหน้าควรต้องมีการลงทะเบียนซ้ำเพื่อเก็บภาพใบหน้าปัจจุบันในระยะเวลาที่ไม่เกิน 6 ปี

(4.4) ลักษณะเฉพาะชีวมิติที่เป็นลักษณะเฉพาะทางสรีรวิทยาประเภทอื่น ๆ เช่น ดีเอ็นเอจะไม่เปลี่ยนแปลงตลอดช่วงอายุขัย ลายเส้นเลือดจะไม่เปลี่ยนแปลงยกเว้นกรณีอุบัติเหตุและเจ็บป่วย

(4.5) ลักษณะเฉพาะชีวมิติที่เป็นลักษณะเฉพาะทางพฤติกรรม มีความไม่คงทน สามารถเปลี่ยนแปลงไปในแต่ละครั้งที่พยายามเก็บข้อมูล เช่น ลายเซ็น เสียงพูด รูปแบบการเดิน โดยเฉพาะเสียงพูดมีการเปลี่ยนแปลงไปตามอายุที่เพิ่มขึ้น

**(5) ความไม่มั่นคง (vulnerability)** ผู้ให้บริการควรพิจารณาลักษณะเฉพาะชีวมิติที่สามารถปลอมแปลงได้ยาก ระบบรู้จำอัตโนมัติและอุปกรณ์เซนเซอร์ควรจะมีความสามารถในการต่อต้านการโจมตีหลอก (presentation attack) และแจ้งเตือนในกรณีที่มีความพยายามในการโจมตีระบบ ควรจะใช้นโยบายควบคู่กับระบบอัตโนมัติ และการเฝ้าตรวจโดยบุคลากร เพื่อที่จะลดการโจมตีและจุดอ่อนตามตำแหน่งต่าง ๆ ที่สามารถจะโจมตีได้ รายละเอียดข้อเสนอแนะเกี่ยวกับการใช้งานชีวมิติและความมั่นคงปลอดภัยจะอยู่ในหัวข้อที่ 7 ของมาตรฐานเล่มนี้

**(6) ความเป็นส่วนตัว (privacy)** ผู้ให้บริการควรพิจารณาลักษณะเฉพาะชีวมิติในประเด็นความเป็นส่วนตัวด้วย การเก็บข้อมูลอัตลักษณ์ที่เกี่ยวกับความเป็นส่วนตัวต้องได้รับความยินยอมจากเจ้าของเพราะเป็นข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [10] รายละเอียดข้อเสนอแนะเกี่ยวกับการใช้งานชีวมิติและสิทธิส่วนบุคคลจะอยู่ในหัวข้อที่ 8 ของมาตรฐานเล่มนี้ ข้อควรระวังสำหรับลักษณะเฉพาะชีวมิติบางประเภทที่มีความเกี่ยวข้องกับความเป็นส่วนตัว มีดังต่อไปนี้

(6.1) ใบหน้า การเลือกใช้ลักษณะเฉพาะชีวมิติประเภทนี้ต้องระวังความเป็นส่วนตัว เนื่องจากมนุษย์สามารถรู้จำใบหน้าบุคคลผู้มีชื่อเสียงหรือเป็นที่รู้จักได้ ทำให้เจ้าหน้าที่ผู้เกี่ยวข้องรู้จักเจ้าของระเบียนจากใบหน้าและสามารถเข้าไปดูข้อมูลส่วนบุคคลของบุคคลเหล่านี้ได้ ซึ่งเป็นการละเมิดสิทธิส่วนบุคคล

(6.2) ดีเอ็นเอ การเลือกใช้ลักษณะเฉพาะชีวมิติประเภทนี้จะมีความเสี่ยงเกี่ยวกับความเป็นส่วนตัวสูงมาก เนื่องจากข้อมูลดีเอ็นเอสามารถตรวจสอบความสัมพันธ์ระหว่างบุคคลได้ ซึ่งละเมิดสิทธิส่วนบุคคลในกรณีที่เจ้าของชีวมิติไม่อนุญาต นอกจากนี้ ดีเอ็นเอยังมีความเกี่ยวข้องกับโรคที่เกี่ยวข้องกับพันธุกรรม ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความสำคัญและมีผลกระทบกับความเป็นส่วนตัวเป็นอย่างยิ่ง

**(7) การใช้ลักษณะเฉพาะชีวมิติหลายประเภท (multi-characteristic-type)** ในกรณีที่ลักษณะเฉพาะชีวมิติประเภทเดียวไม่สามารถตอบโจทย์ที่ต้องการจะนำไปประยุกต์ใช้งาน เนื่องจากต้องครอบคลุมประชากรในวงกว้าง ซึ่งต้องรองรับความหลากหลายของบุคคล ควรเลือกใช้ลักษณะเฉพาะชีวมิติหลายประเภทเพื่อรองรับปัญหานี้ ตัวอย่างเช่นในกรณีของการทำบัตรประชาชนของประเทศอินเดีย (Aadhaar) จะใช้ลายนิ้วมือ ม่านตา และใบหน้า รองรับการพิสูจน์ยืนยันตัวตนและระบุตัวตนทั้งหมด 1,200 ล้านคน [11] ข้อดีคือสามารถชดเชยข้อบกพร่องของกันและกันได้ เช่นฝาแฝดที่มีใบหน้าเหมือนกัน แต่มีลายนิ้วมือและลายม่านตาแตกต่างกัน และการรวมกันทำให้สมรรถนะความแม่นยำสูงขึ้น แต่ข้อเสียคือค่าใช้จ่ายในการลงทุนและดูแลรักษาระบบที่สูงขึ้นกว่าเดิมมาก

## 5.2 ข้อควรพิจารณาในการเลือกระบบรู้จำชีวมิติอัตโนมัติ

เมื่อเลือกประเภทของลักษณะเฉพาะชีวมิติแล้ว การเลือกระบบรู้จำชีวมิติอัตโนมัติให้เหมาะสมกับงานเป้าหมายเป็นสิ่งที่สำคัญ หลักในการพิจารณาเลือกระบบรู้จำชีวมิติอัตโนมัติให้เหมาะสมสำหรับการใช้งานมีดังต่อไปนี้

**(1) วิธีการดำเนินงาน (modes of operation)** ผู้ให้บริการควรกำหนดประเภทการทำงานของระบบที่ต้องการ เช่น การยืนยันตัวตน การระบุตัวตน หรือการทำงานลักษณะเฉพาะชีวมิติหลายประเภทรวมกัน ระบบรู้จำชีวมิติอัตโนมัติของแต่ละบริษัทผู้ผลิตอาจมีจุดเด่นที่แตกต่างกัน บางผลิตภัณฑ์อาจมีจุดเด่นทางด้านการยืนยันตัวตน ในขณะที่บางผลิตภัณฑ์อาจเด่นทางด้านการระบุตัวตน

**(2) สมรรถนะ (performance)** ผู้ให้บริการควรเลือกใช้ระบบที่มีสมรรถนะความแม่นยำในการยืนยันตัวตนตามความต้องการ โดยเลือกระบบที่มีสมรรถนะความแม่นยำสูงสุดเท่าที่งบประมาณจะอำนวย ซึ่งสามารถพิจารณาได้จากอัตราความผิดพลาดต่าง ๆ ของระบบเมื่อทดสอบกับฐานข้อมูลที่จะใช้งาน หรือที่ใกล้เคียงกับที่ต้องการใช้งาน เพื่อลดความเสี่ยงในการเกิดปัญหาจากความผิดพลาดของระบบอัตโนมัติซึ่งจะต้องใช้บุคลากรมาแก้ไขปัญหาในภายหลัง การเลือกใช้ระบบที่มีสมรรถนะต่ำจะก่อให้เกิดปัญหาความผิดพลาดซึ่งหมายถึงค่าใช้จ่าย บุคลากร และเวลาในการแก้ไขปัญหา ในกรณีที่ระบบมีสมรรถนะต่ำกว่าเสนอราคาที่ต่ำกว่า ควรพิจารณาประเมินความเสียหายที่ต้องแก้ไขเมื่อระบบผิดพลาดก่อนตัดสินใจเลือกระบบที่มีสมรรถนะต่ำ เพราะเมื่อรวมค่าใช้จ่ายในการแก้ไขปัญหาที่ส่วนใหญ่เป็นปัญหาระยะยาวแล้ว ราคาอาจสูงกว่าระบบที่มีราคาสูงกว่าซึ่งมีสมรรถนะสูงกว่า ซึ่งคุ้มค่ากว่าในระยะยาว

**(3) เวลาการตอบสนอง (response time)** ผู้ให้บริการควรเลือกระบบรู้จำชีวมิติอัตโนมัติที่ทำงานได้เร็วเพียงพอกับความต้องการในวิธีการดำเนินการที่ต้องใช้ ดังต่อไปนี้

(3.1) การยืนยันตัวตน ระบบควรตอบสนองอย่างรวดเร็ว ทันที ในเวลาจริง ซึ่งงานส่วนใหญ่ผู้ใช้ต้องรอผลการตอบสนองจากระบบ

(3.2) การระบุตัวตน ระบบควรตอบสนองในเวลาที่จำกัด และรวดเร็วที่สุดเท่าที่จะเป็นไปได้เนื่องจากมีการรอผลการตอบสนองจากผู้ใช้ การระบุตัวตนสำหรับบริการประชาชนจะถูกใช้ในการลงทะเบียนเพื่อป้องกันการซ้ำซ้อนของบุคคล ซึ่งการตอบสนองอาจต้องใช้เวลาในการค้นหาและตรวจสอบความถูกต้อง ควรเลือกระบบที่ตอบสนองเร็วที่สุดเท่าที่เป็นไปได้ ในกรณีที่สมรรถนะหรือความถูกต้องใกล้เคียงกัน

(3.3) การค้นหาบุคคลเฝ้าระวัง ระบบควรตอบสนองในเวลาที่รวดเร็วที่สุดเท่าที่จะเป็นไปได้เนื่องจากมีการรอผลการตอบสนองจากผู้ใช้ ซึ่งการตอบสนองอาจต้องใช้เวลาในการค้นหาและตรวจสอบความถูกต้องของบุคคลเฝ้าระวัง ควรเลือกระบบที่ตอบสนองเร็วที่สุดเท่าที่เป็นไปได้ ในกรณีที่สมรรถนะหรือความถูกต้องใกล้เคียงกัน

**(4) ค่าใช้จ่าย (cost)** ค่าใช้จ่ายของระบบควรนำมาทำการเปรียบเทียบถ่วงดุลย์กับประโยชน์ที่ได้จากระบบที่สามารถส่งผลในการแก้ปัญหาหรือป้องกันปัญหาที่จะเกิดขึ้นได้ ถ้าค่าใช้จ่ายของระบบรู้จำชีวมิติอัตโนมัติที่จะใช้ดูคลุมเครือและให้ผลประโยชน์น้อยกับระบบทั้งหมด ควรมองหาลักษณะเฉพาะชีวมิติตัวเลือกอื่นจะดีกว่า รวมทั้งควรประเมินค่าใช้จ่ายในการบริหารจัดการและบำรุงรักษาระบบด้วย

**(5) ขนาดของฐานข้อมูล (size of database)** ระบบแต่ละประเภทอาจมีความต้องการการใช้งานขนาดฐานข้อมูลไม่เท่ากัน โดยปกติแล้ว ฐานข้อมูลจะมีการขยายขนาดตามเวลาการใช้งาน ซึ่งขนาดฐานข้อมูลจะมีผลกระทบทั้งประสิทธิภาพ สมรรถนะ และค่าใช้จ่ายในการดูแลรักษา ดังนั้นการเลือกระบบควรคำนึงถึงประสิทธิภาพที่ระบบรับประกันตามขนาดฐานข้อมูลด้วย

**(6) เงื่อนไขในการดำเนินการ (conditions of operation)** ผู้ให้บริการควรเลือกระบบที่มีความทนทานต่อการเปลี่ยนแปลงซึ่งอาจเกิดจากสภาพแวดล้อมต่าง ๆ โดยควรคำนึงถึงสภาพแวดล้อมในการใช้งานที่กระทบกับระบบ เช่น ระบบทำงานอยู่ภายในอาคารหรือภายนอกอาคาร ในบริเวณนั้นมีฝุ่น อุณหภูมิ ความชื้น หรืออยู่ใกล้ทะเลหรือไม่ หากได้รับผลกระทบจากสภาพแวดล้อม อาจต้องพิจารณาใช้อุปกรณ์ที่สามารถทนต่อสภาพแวดล้อมดังกล่าวได้อย่างเหมาะสม ซึ่งหมายถึงค่าใช้จ่ายที่อาจเพิ่มขึ้น

**(7) สถานที่ติดตั้ง (installation location)** ผู้ให้บริการควรคำนึงถึงสถานที่ตั้งอุปกรณ์รับข้อมูลตัวอย่างชีวมิติ โดยผู้ให้บริการควรพิจารณาสถานที่ติดตั้งระบบที่มีผลกระทบกับผู้ใช้ เช่น ระบบรู้จำใบหน้าที่ใช้กับกล้องวงจรปิดเพื่อการตรวจสอบการเข้าทำงาน ต้องติดตั้งในสถานที่เปิดเผยที่ไม่ถูกทำลายหรือหลบเลี่ยงได้ง่าย เนื่องจากผู้ใช้งานอาจรู้สึกเสียผลประโยชน์จากการมีระบบ หรือในกรณีที่ใช้ระบบรู้จำลายนิ้วมือเพื่อตรวจสอบการเข้าทำงานตามเวลากำหนด อาจถูกทำให้ไม่สามารถใช้งานได้

**(8) ผู้ใช้งาน (users)** ผู้ให้บริการควรเลือกใช้ระบบรู้จำชีวมิติอัตโนมัติที่เหมาะสมกับกลุ่มผู้ใช้งาน เช่น ถ้าผู้ใช้เป็นกลุ่มผู้ใช้แรงงานทางด้านการเกษตร งานก่อสร้าง งานประมง ที่ไม่ได้ใส่ถุงมือขณะทำงาน ทำให้ลายนิ้วมือถูกทำลาย จึงไม่ควรเลือกใช้ระบบรู้จำลายนิ้วมือ หรือ ในกรณีที่มีการปกปิดใบหน้าจากหน้ากาก หรือข้อบังคับทางศาสนา ก็ไม่ควรเลือกระบบรู้จำใบหน้า

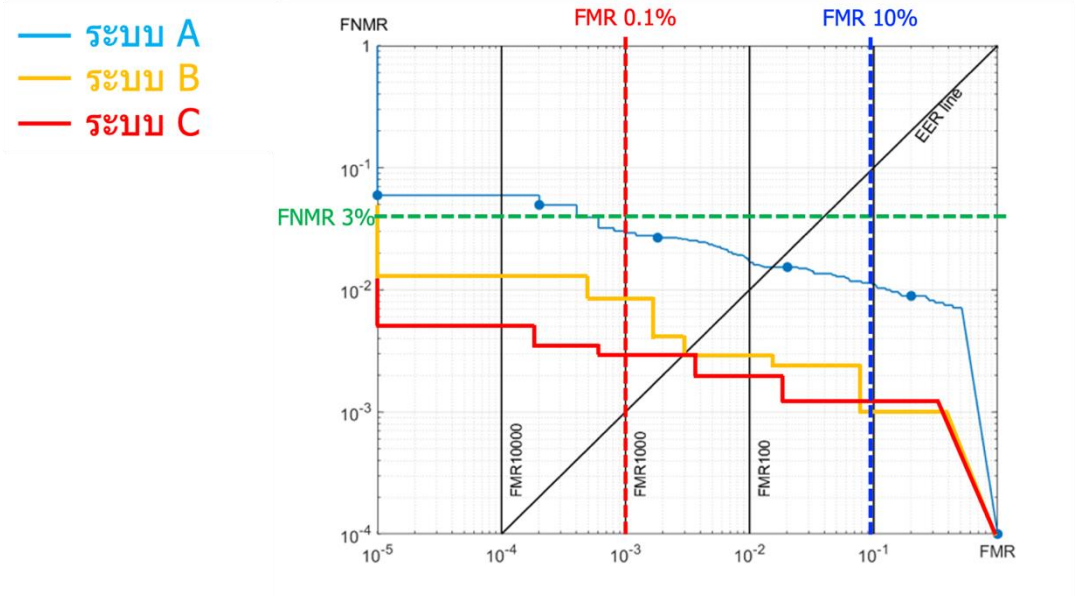
**(9) พฤติกรรมของผู้ใช้งาน (user's behaviors)** ผู้ให้บริการควรพิจารณาการยอมรับของผู้ใช้ และการให้ความร่วมมือจากผู้ใช้ เช่น ในปัจจุบันมีโรคระบาดที่ต้องหลีกเลี่ยงการสัมผัส การใช้ระบบรู้จำชีวมิติ

อัตโนมัติที่ต้องสัมผัส เช่น การสแกนลายนิ้วมืออาจไม่ได้รับการยอมรับจากผู้ใช้ ในขณะที่ระบบรู้จำใบหน้าจะได้รับการยอมรับจากผู้ใช้มากกว่าเนื่องจากไม่ต้องสัมผัส

(10) **การป้องกันการโจมตีหลอก (presentation attack protection)** ผู้ให้บริการควรเลือกระบบที่มีความสามารถในการป้องกันการโจมตีหลอกด้วยเทคโนโลยีปัจจุบันได้ รายละเอียดข้อเสนอแนะเกี่ยวกับการป้องกันการโจมตีหลอกจะอยู่ในหัวข้อที่ 7 ของมาตรฐานเล่มนี้

(11) **สถานที่กู้คืนข้อมูลเมื่อเกิดภัยพิบัติ (disaster recovery site)** ผู้ให้บริการควรมีศูนย์หรือสถานที่บันทึกข้อมูลตัวอย่างชีวมิติไว้ในลักษณะที่บันทึกเก็บข้อมูลโดยให้อ่านเพียงอย่างเดียว (read only) ในลักษณะแคปซูลเวลา (time capsule) ไม่ให้มีการแก้ไขข้อมูลในอดีต และถ้าไม่มีเหตุจำเป็นก็จะไม่อ่านข้อมูลออกมา เมื่อเกิดภัยพิบัติหรือมีปัญหากับระบบปัจจุบัน สามารถอ่านข้อมูลออกมา เพื่อกู้ระบบหรือเปลี่ยนระบบเป็นระบบรู้จำชีวมิติอัตโนมัติใหม่ได้โดยไม่เสียข้อมูลอ้างอิงชีวมิติในอดีต

ตัวอย่างการพิจารณาเลือกระบบโดยการเปรียบเทียบสมรรถนะของระบบ เช่น การเปรียบเทียบประสิทธิภาพของระบบการพิสูจน์ยืนยันตัวตนจะพิจารณาจากอัตราการเข้าคู่ผิดพลาดหรือ FMR (false match rate) และอัตราการไม่เข้าคู่ผิดพลาด FNMR (false non-match rate) ที่ทดสอบด้วยชุดข้อมูลตัวอย่างชีวมิติที่ใกล้เคียงกับการใช้งานจริงให้มากที่สุด เช่น ระบบพิสูจน์ยืนยันตัวตนด้วยใบหน้าจากในหนังสือเดินทางเปรียบเทียบกับใบหน้าของผู้ถือหนังสือเดินทาง ชุดข้อมูลทดสอบก็ต้องใช้ภาพใบหน้าที่มีลักษณะเฉพาะเหมือนกับที่ได้จากหนังสือเดินทาง และภาพใบหน้าที่ถ่ายได้จากผู้ถือหนังสือเดินทางที่จุดแสดงตนในสถานที่เดินทาง ตัวอย่างการเปรียบเทียบประสิทธิภาพแสดงได้ดังรูปที่ 3




**รูปที่ 3 กราฟเส้นโค้งการแลกเปลี่ยนการตรวจจับที่ผิดพลาด หรือ DET (detection-error tradeoff) ที่แสดงประสิทธิภาพของระบบชีวมิติ A B และ C สำหรับการยืนยันตัวตน**

จากกราฟหากพิจารณาในภาพรวมจะเห็นว่าระบบรู้จำชีวมิติอัตโนมัติ C (เส้นสีแดง) มีประสิทธิภาพโดยรวมสูงกว่าระบบรู้จำชีวมิติอัตโนมัติ A (เส้นสีฟ้า) และ ระบบรู้จำชีวมิติอัตโนมัติ B (เส้นสีเหลือง) ซึ่งหากกำหนดประสิทธิภาพขั้นต่ำของระบบที่ต้องการใช้ที่อัตราการไม่เข้าคู่ผิดพลาด FNMR น้อยกว่าหรือเท่ากับ 3% (เส้นประสีเขียว) และอัตราการเข้าคู่ผิดพลาด FMR น้อยกว่าหรือเท่ากับ 0.1% (เส้นประสีแดง) ระบบที่ควร

เลือกใช้คือ ระบบรู้จำชีวมิติอัตโนมัติ C (เส้นสีแดง) เนื่องจากมีเส้นกราฟ DET ต่ำกว่าทุกระบบ ซึ่งหมายถึงความผิดพลาดที่ต่ำกว่าทุกระบบ

ถ้ากำหนดที่อัตราการเข้าคู่ผิดพลาด FMR เท่ากับ 10% (เส้นประสีน้ำเงิน) ระบบที่ควรเลือกใช้อาจเป็นระบบรู้จำชีวมิติอัตโนมัติ B หรือ ระบบรู้จำชีวมิติอัตโนมัติ C ก็ได้ ซึ่งในกรณีนี้ควรคำนึงถึงปัจจัยอื่น ๆ ที่เกี่ยวข้องในการเลือกใช้ระบบรู้จำชีวมิติอัตโนมัติดังที่กล่าวมาข้างต้น แต่หากพิจารณาเพียงกราฟ DET ปัจจัยเดียวระบบที่ควรเลือกใช้คือระบบรู้จำชีวมิติอัตโนมัติ C เนื่องจากมีค่าเฉลี่ยบริเวณ FMR เท่ากับ 10% ต่ำกว่าระบบรู้จำชีวมิติอัตโนมัติ B แม้ว่าที่ตำแหน่ง FMR เท่ากับ 10% ระบบรู้จำชีวมิติอัตโนมัติ B จะมีค่าผิดพลาดต่ำกว่าระบบรู้จำชีวมิติอัตโนมัติ C

## 5.3 ข้อควรระวังเกี่ยวกับการเก็บและการบันทึกข้อมูลชีวมิติ

ข้อมูลชีวมิติหรือข้อมูลชีวภาพถือเป็นข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [10] การเก็บข้อมูลชีวมิติจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน จึงจะสามารถเก็บข้อมูลชีวมิติได้ ผู้ให้บริการซึ่งเป็นผู้เก็บข้อมูลชีวมิติจะต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมและการใช้งานข้อมูลชีวมิติไว้อย่างชัดเจนให้เข้าใจได้โดยง่าย เพื่อให้เจ้าของข้อมูลรับทราบและให้ความยินยอม โดยสาเหตุของการเก็บข้อมูลชีวมิติโดยทั่วไปแล้ว มีดังต่อไปนี้

(1) **การพิสูจน์ยืนยันชีวมิติ** เพื่อใช้พิสูจน์ยืนยันตัวตน โดยอ้างอิงจากนิยามที่ให้ไว้ในหัวข้อที่ 4 (1)

(2) **การระบุชีวมิติ** เพื่อใช้ระบุตัวตน โดยอ้างอิงจากนิยามที่ให้ไว้ในหัวข้อที่ 4 (2)

(3) **การแก้ปัญหาในกรณีที่ระบบรู้จำชีวมิติอัตโนมัติทำงานผิดพลาด** ในกรณีที่ผู้ใช้บริการร้องเรียนว่าถูกปฏิเสธการยืนยันตัวตนโดยระบบรู้จำชีวมิติอัตโนมัติ แต่ผู้ใช้ยืนยันว่าเป็นเจ้าของอัตลักษณ์จริง ๆ มีความจำเป็นที่ต้องพิสูจน์ยืนยันตัวตน โดยสามารถเรียกข้อมูลอ้างอิงชีวมิติที่บันทึกไว้มาพิจารณาเปรียบเทียบกับข้อมูลตัวอย่างชีวมิติที่ได้จากผู้ใช้บริการในขณะนั้น โดยเจ้าหน้าที่ต้องมีความเชี่ยวชาญในการพิจารณาเปรียบเทียบข้อมูลอ้างอิงชีวมิติกับข้อมูลตัวอย่างชีวมิติเพื่อสามารถตัดสินใจได้ว่าใช่คน ๆ เดียวกันหรือไม่ใช่ เพื่อให้ผู้ใช้บริการสามารถทำธุรกรรมต่อไปได้

(4) **การป้องกันปัญหาข้อมูลชีวมิติมีการเปลี่ยนแปลง** ข้อมูลชีวมิติอาจมีการเปลี่ยนแปลงได้ตามธรรมชาติหรือการจงใจทำให้เกิดการเปลี่ยนแปลง ผู้ให้บริการอาจมีความจำเป็นต้องเก็บและบันทึกข้อมูลตัวอย่างชีวมิติไว้เป็นหลักฐานตามความจำเป็นที่ผู้ใช้บริการเข้าใช้งานระบบรู้จำชีวมิติอัตโนมัติ โดยเก็บและบันทึกข้อมูลตัวอย่างชีวมิติในแต่ละช่วงเวลาในรูปแบบระเบียนที่สามารถทำการตรวจสอบย้อนหลังได้ในกรณีที่ข้อมูลตัวอย่างชีวมิติเกิดการเปลี่ยนแปลง ซึ่งจะทำให้สามารถระบุสาเหตุการเปลี่ยนแปลงที่เกิดจากธรรมชาติ เช่นการเกิดอุบัติเหตุ หรือ การเปลี่ยนแปลงอย่างจงใจ เช่น การผ่าตัดศัลยกรรมใบหน้า หรือการจงใจเปลี่ยนแปลงลายนิ้วมือ นอกจากนี้ เพื่อป้องการเปลี่ยนแปลงแก้ไขโดยมิชอบจากเจ้าหน้าที่ที่อาจร่วมมือกับอาชญากรในการสวมตัวผู้ใช้บริการด้วยการลงทะเบียนข้อมูลตัวอย่างชีวมิติใหม่ทับข้อมูลอ้างอิงชีวมิติเดิม การเก็บและบันทึกข้อมูลตัวอย่างชีวมิติในลักษณะนี้จะป้องกันการถูกสวมตัวในอนาคต

(5) **การแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน** ในกรณีที่มีความจำเป็นต้องแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงานที่ทำงานเกี่ยวข้องประสานความร่วมมือกัน เนื่องจากแต่ละหน่วยงานอาจใช้งานระบบรู้จำชีวมิติอัตโนมัติต่างผู้ผลิต การแลกเปลี่ยนระหว่างระบบที่แตกต่างกันจะต้องแลกเปลี่ยนด้วยข้อมูล

ตัวอย่างชีวมิติ โดยเฉพาะในงานทางด้านนิติวิทยาศาสตร์ซึ่งมีความจำเป็นต้องพิจารณาข้อมูลตัวอย่างชีวมิติเป็นหลักในการทำงาน

(6) **การปรับปรุงพัฒนาและทดสอบสมรรถนะของระบบ** เพื่อพัฒนาระบบฯ ให้สามารถทำงานได้อย่างเต็มประสิทธิภาพ ผู้ให้บริการอาจมีความจำเป็นต้องเก็บและบันทึกข้อมูลตัวอย่างชีวมิติไว้สำหรับทดสอบสมรรถนะของระบบ ฯ ซึ่งจะต้องใช้ข้อมูลตัวอย่างชีวมิติจำนวนมากในการทดสอบสมรรถนะที่แท้จริงของระบบ ฯ รวมทั้งการทดสอบวัดคุณภาพของข้อมูลตัวอย่างชีวมิติในปัจจุบันเพื่อการปรับปรุงการเก็บข้อมูลตัวอย่างชีวมิติให้มีคุณภาพดีขึ้นในอนาคต ทั้งหมดนี้เพื่อพัฒนาปรับปรุงงานบริการที่ใช้ระบบรู้จำชีวมิติอัตโนมัติให้มีประสิทธิภาพสูงสุด

(7) **การแก้ปัญหาในกรณีที่ต้องเริ่มระบบรู้จำชีวมิติอัตโนมัติใหม่ทั้งหมด** เช่น ในกรณีการเปลี่ยนซอฟต์แวร์รู้จำชีวมิติอัตโนมัติต่างผู้ผลิต การเปลี่ยนผู้รับจ้างดูแลระบบในกรณีที่ผู้รับจ้างเดิมหมดสัญญาหรือไม่สามารถทำงานต่อไปได้ การเก็บข้อมูลอ้างอิงชีวมิติที่อยู่ในรูปแบบมาตรฐานจะทำให้สามารถกู้ฐานข้อมูลอ้างอิงชีวมิติและสร้างระบบรู้จำชีวมิติอัตโนมัติขึ้นมาใหม่ทั้งหมดได้ และสามารถใช้งานต่อไปได้อย่างต่อเนื่องโดยไม่ต้องสูญเสียข้อมูลชีวมิติเดิม

ในการเก็บข้อมูลตัวอย่างชีวมิติอาจมีนำไปใช้ในกรณีต่าง ๆ ตามที่ได้กล่าวไว้ทั้ง 7 ข้อ หรืออาจมีการนำไปใช้ตามความจำเป็นอื่นที่ไม่ได้กำหนดไว้ในข้อเสนอแนะมาตรฐานนี้ แต่ต้องระบุสาเหตุอื่น ๆ เหล่านี้ไว้ให้เจ้าของข้อมูลรับทราบและยินยอม ในกรณีการใช้งานตามข้อที่ (1) เพียงอย่างเดียว อาจไม่จำเป็นต้องบันทึกข้อมูลตัวอย่างชีวมิติเก็บไว้ในฐานข้อมูลและไม่จำเป็นที่จะต้องแสดงข้อมูลตัวอย่างชีวมิติในจอภาพ ในกรณีการใช้งานข้อ (2) อาจมีความจำเป็นที่จะต้องใช้ข้อมูลตัวอย่างชีวมิติมาแสดงในจอภาพเพื่อเปรียบเทียบกับข้อมูลอ้างอิงชีวมิติประกอบกับการพิจารณาของเจ้าหน้าที่ เพื่อให้สามารถทำงานระบุตัวตน ให้สำเร็จลุล่วงไปได้ด้วยดี สำหรับในกรณีการใช้งานตั้งแต่ข้อ (2), (3), (4), (5), (6), (7) อาจมีความจำเป็นต้องบันทึกข้อมูลอ้างอิงชีวมิติสำหรับการใช้ในงานต่าง ๆ ดังกล่าว และในกรณี (3), (4), (5), (6), (7) อาจต้องบันทึกข้อมูลตัวอย่างชีวมิติที่ได้จากผู้ใช้บริการในขณะนั้นด้วย ดังนั้นผู้ให้บริการต้องขอความยินยอมจากเจ้าของข้อมูลชีวมิติโดยให้เหตุผลประกอบอย่างชัดเจน

การเก็บและบันทึกข้อมูลชีวมิติหรือข้อมูลชีวภาพ ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [10]

เมื่อผู้ใช้บริการยกเลิกการใช้บริการ หรือขอถอนความยินยอมในการเก็บรวบรวม ใช้ข้อมูลชีวมิติ ผู้ให้บริการจะต้องดำเนินการลบหรือทำลายข้อมูลอัตลักษณ์บุคคลทั้งหมดรวมทั้งข้อมูลชีวมิติ หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [10]

## 5.4 ข้อควรพิจารณาในการกำหนดบทบาทของบุคลากรกับระบบรู้จำชีวมิติอัตโนมัติ

เมื่อต้องการใช้ระบบรู้จำชีวมิติอัตโนมัติใน IdMS ผู้ให้บริการควรพิจารณาการกำหนดบทบาทของบุคลากรที่ต้องทำงานร่วมกับระบบรู้จำชีวมิติอัตโนมัติเพื่อให้เกิดประสิทธิผลสูงสุดตามเป้าหมายที่วางไว้ ระบบรู้จำชีวมิติอัตโนมัติเป็นเพียงเครื่องมือที่ช่วยเพิ่มระดับความมั่นใจในการพิสูจน์ยืนยันตัวตน เนื่องจากระบบ

สามารถทำงานผิดพลาดได้ ดังนั้นจำเป็นต้องมีบุคลากรที่มีความเชี่ยวชาญช่วยแก้ปัญหาในส่วนที่ระบบทำงานผิดพลาด โดยมีข้อควรพิจารณาดังต่อไปนี้

(1) ผู้ให้บริการควรพิจารณาบทบาทของบุคลากรกับผลลัพท์ที่ต้องการ โดยพิจารณาว่า บุคลากรมีข้อควรปฏิบัติต่อกระบวนการต่าง ๆ ในระบบรู้จำชีวมิติอัตโนมัติอย่างไร โดยเฉพาะ การลงทะเบียน การตรวจคุณภาพของภาพหรือข้อมูลตัวอย่างชีวมิติ การพิสูจน์ยืนยันตัวตน และการระบุตัวตน เนื่องจากการพิสูจน์ยืนยันตัวตนและระบุตัวตนกับระบบอัตโนมัตินั้นไม่สมบูรณ์แบบ บทบาทของบุคลากรจะมีส่วนช่วยแก้ไขในส่วนที่ระบบอัตโนมัติเกิดความผิดพลาด เพื่อให้สามารถทำงานตามหน้าที่ได้อย่างสมบูรณ์

(2) ผู้ให้บริการควรพิจารณาว่า ใครได้รับอนุญาตในการเห็นผลการเปรียบเทียบหรือการพิจารณาดูข้อมูลตัวอย่างชีวมิติ และการแก้ไขข้อผิดพลาดที่เกิดจากระบบ รวมทั้งควรพิจารณาแนวทางการแก้ปัญหาที่แตกต่างกันสำหรับแต่ละผังระบบงานสำหรับบุคลากร โดยองค์กรควรพิจารณาครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้

   (2.1) คุณสมบัติของบุคลากร การฝึกอบรม การพัฒนาขีดความสามารถ

   (2.2) ลักษณะหน้าจอการแสดงผล (GUI)

   (2.3) ผังระบบงาน หรือขั้นตอนการประมวลผลสำหรับการเปรียบเทียบ การลงทะเบียน การพิสูจน์ยืนยันตัวตน และการระบุตัวตน

   (2.4) การจัดการข้อยกเว้น หรือ กรณีพิเศษ หรือกรณีที่เกิดปัญหา

   (2.5) คุณภาพของข้อมูลที่ต้องการสำหรับกระบวนการเปรียบเทียบข้อมูลชีวมิติ

## 5.5 ข้อเสนอแนะในการสร้างความเชื่อมั่นในการรวมกันของฐานข้อมูล

การนำระบบรู้จำชีวมิติอัตโนมัติใหม่เข้ามาใช้ในระบบ IdMS เดิมที่มีระบบรู้จำชีวมิติอัตโนมัติเก่าอยู่ก่อนหน้าแล้วหรือยังไม่มีระบบอยู่ก่อนหน้าก็ตาม ก่อนที่จะมีการรวมกันของฐานข้อมูลของระบบเก่ากับระบบใหม่ หรือ ก่อนที่จะมีการนำข้อมูลจากหน่วยงานอื่นเข้ามารวมกันในระบบ IdMS ควรมีกระบวนการสร้างความเชื่อมั่นในการนำข้อมูลของระบบเก่าและระบบใหม่มารวมกัน [6] มีข้อเสนอแนะดังต่อไปนี้

(1) ผู้ให้บริการต้องมีกระบวนการทำความสะอาดข้อมูล (data cleansing process) หรือทำให้ข้อมูลอยู่ในคุณภาพตามมาตรฐานเดียวกัน กระบวนการนี้มีความสำคัญมากและควรนำไปปฏิบัติให้เกิดผล เนื่องจากมีผลกระทบกับสมรรถนะของระบบในระยะยาว

(2) ในกรณีที่ข้อมูลมีความขัดแย้งกัน จะทำให้เกิดปัญหาใหญ่ตามมาที่จะทำให้การทำงานของ IdMS ล้มเหลว เช่น บุคคลเดียวมีตัวระบุอัตลักษณ์ที่ไม่ใช่ข้อมูลชีวมิติมากกว่าหนึ่ง (ตัวอย่างเช่น บุคคลเดียวมีเลขประจำตัวหลายตัวเลข) หรือ บุคคลหลายคนใช้ตัวระบุอัตลักษณ์ตัวเดียวกัน (ตัวอย่างเช่น มีผู้ใช้เลขประจำตัวร่วมกันมากกว่าหนึ่ง) สถานการณ์เหล่านี้เกิดขึ้นได้เนื่องจาก ความผิดพลาดของมนุษย์ ระบบผิดพลาด กระบวนการล้มเหลว หรือ สาเหตุเพราะการทุจริต

(3) ส่วนหนึ่งของกระบวนการที่ทำให้เกิดความมั่นใจของการรวมกันของฐานข้อมูล องค์กรหรือผู้ให้บริการควรรู้ว่าจะมีข้อมูลที่ถูกสร้างขึ้นในปริมาณมาก และอาจต้องใช้ระยะเวลานานในการจัดการข้อมูลจนกว่าระบบจะสามารถทำงานได้ตามความประสงค์

(4) ในกรณีที่องค์กรหรือผู้ให้บริการรับข้อมูลตัวอย่างชีวมิติจากหน่วยงานอื่นหรือผู้ให้บริการอื่น ซึ่งมีกระบวนการลงทะเบียนชีวมิติที่มีมาตรฐานต่ำกว่ามาตรฐานขององค์กรหรือหน่วยงานของตนเอง ควรจะต้องระมัดระวังความเสี่ยงที่เกิดขึ้นจากข้อมูลตัวอย่างชีวมิติที่นำเข้า และต้องตรวจวัดคุณภาพตามความจำเป็น

## 6. ข้อเสนอแนะเกี่ยวกับการใช้เทคโนโลยีชีวมิติสำหรับการบริหารอัตลักษณ์บุคคล

สำหรับบทนี้จะเป็นข้อเสนอแนะที่มีรายละเอียดเกี่ยวกับการใช้เทคโนโลยีชีวมิติสำหรับการบริหารอัตลักษณ์บุคคล โดยเฉพาะในส่วนที่สำคัญ เพื่อให้เกิดประสิทธิภาพสูงสุด มีความแม่นยำ และเป็นที่เชื่อถือได้ โดยพิจารณาประเด็นต่าง ๆ ที่เกี่ยวข้อง คือ

(1) ข้อเสนอแนะภาพรวมการเก็บข้อมูลชีวมิติ

(2) มาตรฐานการบันทึกข้อมูลชีวมิติ

(3) มาตรฐานการวัดคุณภาพข้อมูลชีวมิติ

(4) มาตรฐานการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน

(5) แนวทางการจัดการข้อมูลชีวมิติและข้อมูลอื่น

(6) ข้อยกเว้นอื่น ๆ

โดยมีรายละเอียดของแต่ละหัวข้อ ดังต่อไปนี้

### 6.1 ข้อเสนอแนะภาพรวมการเก็บข้อมูลชีวมิติ

กระบวนการเก็บข้อมูลชีวมิติ เป็นกระบวนการที่มีความสำคัญอย่างมากในการใช้เทคโนโลยีชีวมิติสำหรับการบริหารอัตลักษณ์บุคคล กระบวนการเก็บข้อมูลชีวมิติที่ดีจะส่งผลโดยตรงต่อความแม่นยำของระบบ IdMS และการใช้งานที่มีประสิทธิภาพสูงสุด โดยมีข้อเสนอแนะที่จำเป็นต้องคำนึงถึง มีดังต่อไปนี้

**(1) อุปกรณ์การเก็บข้อมูลชีวมิติ** อุปกรณ์หรือเซนเซอร์ที่ใช้ในการเก็บข้อมูลตัวอย่างชีวมิติแต่ละประเภทต้องผ่านมาตรฐานที่กำหนด ทำให้สามารถเก็บข้อมูลตัวอย่างชีวมิติที่มีคุณภาพดี อุปกรณ์มีความทนทาน ใช้งานสะดวก และมีความปลอดภัย รายละเอียดของอุปกรณ์หรือเซนเซอร์ที่ใช้เก็บข้อมูลตัวอย่างชีวมิติแต่ละประเภท จะถูกจำแนกกำหนดโดยมาตรฐานเฉพาะของแต่ละลักษณะเฉพาะชีวมิติ ซึ่งเป็นมาตรฐานที่กำหนดต่อจากมาตรฐานนี้

**(2) การวัดคุณภาพข้อมูลชีวมิติ** เมื่อได้รับข้อมูลตัวอย่างชีวมิติผ่านอุปกรณ์เซนเซอร์ ผู้ให้บริการต้องวัดคุณภาพของข้อมูลตัวอย่างชีวมิติก่อนที่จะนำไปบันทึกเก็บหรือใช้งาน และควรเก็บค่าคุณภาพไว้กับข้อมูลชีวมิติ คุณภาพข้อมูลตัวอย่างชีวมิติที่ดี ส่งผลให้ระบบสามารถทำงานได้เต็มประสิทธิภาพ มีความแม่นยำสูงและมีความน่าเชื่อถือ

**(3) การบันทึกข้อมูลชีวมิติ** ข้อมูลตัวอย่างชีวมิติที่เก็บได้ต้องสามารถบันทึกในรูปแบบมาตรฐาน เพื่อให้สามารถนำกลับมาใช้ได้เมื่อต้องการปรับปรุงระบบ การเริ่มระบบใหม่ การตรวจสอบข้อมูลตัวอย่างชีวมิติ การถ่ายโอนระบบ และการแลกเปลี่ยนข้อมูลตัวอย่างชีวมิติในอนาคต ตามรายละเอียดในหัวข้อ 5.3

**(4) สภาพแวดล้อมในการเก็บ** การเก็บข้อมูลตัวอย่างชีวมิติต้องควบคุมปัจจัยของการเก็บข้อมูลเพื่อให้ได้

ข้อมูลตัวอย่างชีวมิติที่มีคุณภาพสมบูรณ์ที่สุด ได้แก่ ในกรณีที่ข้อมูลตัวอย่างชีวมิติเป็นภาพ ต้องควบคุมอุปกรณ์รับภาพ พื้นหลัง การจัดแสง ความสะอาด และความปลอดภัยโดยรอบพื้นที่ของการรับภาพ หรือในกรณีที่เป็นเสียง ต้องควบคุมอุปกรณ์รับเสียง สภาพแวดล้อม เสียงสะท้อน และสัญญาณรบกวน

(5) **ความเสถียรของกระบวนการเก็บและสามารถทำซ้ำได้** การเก็บข้อมูลตัวอย่างชีวมิติต้องจัดหาและเลือกใช้วิธีการเก็บข้อมูลตัวอย่างชีวมิติที่มีความเสถียรและสามารถทำซ้ำได้ โดยข้อมูลตัวอย่างชีวมิติที่เก็บได้ต้องมีคุณภาพสูงที่สุดเท่าที่เป็นไปได้ สามารถทนทานต่อการเปลี่ยนแปลงของปัจจัยภายนอกต่าง ๆ ได้แก่ การเปลี่ยนแปลงของปริมาณแสง การเปลี่ยนแปลงของอุณหภูมิ ความชื้น สิ่งรบกวนภายนอก และตำแหน่งการจัดวางเครื่องสแกนชีวมิติ

(6) **การเก็บข้อมูลชีวมิติระยะไกล** ในกรณีที่ต้องมีการเก็บข้อมูลตัวอย่างชีวมิติจากระยะไกล ควรมีการกำหนดแนวทางปฏิบัติสำหรับการเก็บข้อมูลจากระยะไกล เช่น กรณีของการใช้งานผ่านระบบออนไลน์ซึ่งต้องควบคุมเพื่อป้องกันการโจมตีหลอก หรือกรณีเกิดภัยพิบัติซึ่งผู้ใช้หรือเจ้าหน้าที่ไม่สามารถดำเนินการเก็บข้อมูลตัวอย่างชีวมิติด้วยวิธีปกติได้ ผู้ให้บริการต้องมีแนวทางปฏิบัติยามฉุกเฉินเพื่อให้สามารถดำเนินการเก็บข้อมูลได้ เช่น กรณีภัยสินามิที่ภาคใต้ปีพ.ศ. 2547

(7) **ความล้มเหลวในการเก็บข้อมูลชีวมิติ** ในกรณีที่เกิดความล้มเหลวในการเก็บข้อมูลตัวอย่างชีวมิติ ควรมีการกำหนดขั้นตอนเพิ่มเติมหากเกิดความล้มเหลวในการเก็บข้อมูลหรือการประมวลผลข้อมูลตัวอย่างชีวมิติ เช่น ไม่สามารถเก็บลายนิ้วมือได้เนื่องจากนิ้วมือลอก เป็นแผล หรือ ทำงานบางอย่างที่ลายนิ้วมือถูกทำลาย ควรมีขั้นตอนแก้ปัญหาเหล่านี้ไว้ก่อนล่วงหน้า

(8) **สภาพหรือพฤติกรรมของผู้ใช้** ปัจจัยภายในของมนุษย์ในด้านต่าง ๆ เช่น อารมณ์ ความอ่อนล้า สุขภาพ ความเครียด สามารถส่งผลถึงคุณภาพของการเก็บข้อมูลตัวอย่างชีวมิติ ดังนั้น การเก็บข้อมูลตัวอย่างชีวมิติ ควรคำนึงถึงปัจจัยภายในของมนุษย์ในการเก็บข้อมูลของผู้ใช้ที่จะมีผลกับข้อมูลตัวอย่างชีวมิติ โดยเฉพาะข้อมูลตัวอย่างชีวมิติเชิงพฤติกรรม การเลือกวิธีการเก็บข้อมูลตัวอย่างชีวมิติต้องคำนึงถึงสภาพหรือพฤติกรรมของร่างกายที่สามารถส่งผลถึงลักษณะข้อมูลชีวมิติที่อาจเปลี่ยนแปลงได้ ตัวอย่างเช่นรู้จำใบหน้า จะมีผลกระทบต่อมุมการถ่ายใบหน้า การแสดงออกทางสีหน้า สภาพผิวหนัง หรือผลกระทบจากอุบัติเหตุ จากการเจ็บป่วยและการรักษา

(9) **การเก็บข้อมูลชีวมิติเพื่อการลงทะเบียน** ผู้ให้บริการต้องให้ความสำคัญกับการเก็บข้อมูลตัวอย่างชีวมิติในการลงทะเบียนเป็นครั้งแรกเพื่อนำเข้าข้อมูลชีวมิติ ข้อมูลตัวอย่างชีวมิติควรมีความสมบูรณ์ที่สุดเท่าที่สามารถจะเก็บได้ เนื่องจากยังไม่มีข้อมูลอ้างอิงชีวมิติในระบบรู้จำชีวมิติอัตโนมัติหรือในฐานข้อมูลของผู้ให้บริการมาก่อน ผู้ให้บริการต้องพิสูจน์ยืนยันตัวตนของผู้ใช้บริการอย่างละเอียดถี่ถ้วน ให้สามารถมั่นใจได้ว่าบุคคลนั้นเป็นเจ้าของอัตลักษณ์ดังที่กล่าวอ้างจริง จากนั้นจึงเก็บข้อมูลตัวอย่างชีวมิติซึ่งควรเป็นแบบพบหน้ากับเจ้าหน้าที่ในสภาพแวดล้อมที่ผู้ให้บริการจัดไว้ให้ เพื่อป้องกันการสวมตัวหรือสลับตัว หรือสลับเปลี่ยนชีวมิติหลอกระบบ

(10) **การระบุตัวตนก่อนเก็บข้อมูลชีวมิติในการลงทะเบียน** ต้องป้องกันความซ้ำซ้อนในกรณีที่หนึ่งอัตลักษณ์อ้างอิงมีได้เพียงบุคคลเดียว ต้องทำการค้นหาแบบระบุตัวตนด้วยข้อมูลตัวอย่างชีวมิติที่เก็บได้เพื่อการลงทะเบียนก่อนทุกครั้ง และรับลงทะเบียนและออกหลักฐานแสดงตนได้เมื่อมั่นใจว่าบุคคลที่ลงทะเบียนนี้ไม่ซ้ำซ้อนกับบุคคลที่มีอยู่ในฐานข้อมูลก่อนหน้าเท่านั้น

**(11) การเก็บและบันทึกข้อมูลอ้างอิงชีวมิติต้นฉบับจากการลงทะเบียน** ต้องเก็บและบันทึกข้อมูลอ้างอิงชีวมิติต้นฉบับให้มีความปลอดภัยสูงสุด ต้องมีนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลอ้างอิงชีวมิติที่ชัดเจน ระบบจัดเก็บข้อมูลอ้างอิงชีวมิติต้องอยู่ในเครือข่ายภายในที่ปลอดภัยและต้องรับส่งข้อมูลอ้างอิงชีวมิติผ่านช่องทางที่ปลอดภัย ควรเข้ารหัสข้อมูลอ้างอิงชีวมิติต้นฉบับเพื่อป้องกันคุ้มครองข้อมูลส่วนบุคคล และต้องจำกัดการเข้าถึงข้อมูลส่วนนี้โดยเจ้าหน้าที่ผู้รับผิดชอบเท่านั้น การใช้งานข้อมูลอ้างอิงชีวมิติต้นฉบับควรใช้ในกรณีพิเศษที่สำคัญเช่น การพิสูจน์ตัวตนในกรณีที่มีปัญหาการปฏิเสธการยืนยันตัวตนโดยระบบรู้จำชีวมิติอัตโนมัติ การเริ่มสร้างระบบรู้จำชีวมิติอัตโนมัติใหม่โดยใช้ข้อมูลอ้างอิงชีวมิติเดิม การป้องกัน การแลกเปลี่ยน การปรับปรุง ดังที่กล่าวไว้ในหัวข้อ 5.3 ตามความจำเป็น

**(12) จำนวนข้อมูลชีวมิติต่อบุคคล** เนื่องจากจำนวนข้อมูลชีวมิติแต่ละประเภท อาจมีมากกว่าหนึ่ง เช่น ลายม่านตามีสองข้าง ลายนิ้วมือมีสิบนิ้ว ผู้ให้บริการควรเก็บจำนวนข้อมูลชีวมิติตามความจำเป็นในการใช้งาน เช่น ในกรณีงานทางด้านบริการประชาชน ควรเก็บข้อมูลเท่าที่จำเป็นเช่น การเก็บลายนิ้วมือควรเก็บลายนิ้วมือเพียงสองนิ้วจากสิบนิ้วก็เพียงพอในการยืนยันตัวตน ในกรณีงานทางด้านนิติวิทยาศาสตร์หรือการพิสูจน์ตัวตน การเพิ่มจำนวนข้อมูลชีวมิติจะช่วยให้การระบุตัวตนแม่นยำยิ่งขึ้น จึงควรเก็บลายนิ้วมือทั้งสิบนิ้ว

**(13) ข้อควรระวังเกี่ยวกับอายุข้อมูลชีวมิติ** คุณลักษณะเฉพาะชีวมิติจะมีคุณภาพเปลี่ยนไปตามเวลา และเปลี่ยนไปตามอายุของบุคคล ดังนั้น การเก็บข้อมูลชีวมิติ ควรกำหนดระยะเวลาที่เหมาะสมของการเก็บข้อมูลชีวมิติในฐานข้อมูล และกำหนดให้ผู้ใช้ทำการลงทะเบียนซ้ำ เพื่อปรับปรุงข้อมูลให้ได้ข้อมูลชีวมิติปัจจุบัน เพื่อลดความผิดพลาดของการพิสูจน์ยืนยันตัวตนหรือการระบุตัวตน

**(14) ความปลอดภัยในการเก็บข้อมูลตัวอย่างชีวมิติ** ช่วงการเก็บข้อมูลตัวอย่างชีวมิติจะเป็นจุดที่ถูกโจมตีหลอกได้ง่ายที่สุด ภาพชีวมิติต้นฉบับหรือข้อมูลตัวอย่างชีวมิติที่จัดเก็บต้องมีระบบที่มีการจัดการรักษาความปลอดภัยของข้อมูลชีวมิติอย่างเข้มงวด เพื่อรักษาความลับของข้อมูลชีวมิติแก่ผู้ใช้บริการ และป้องกันการโจมตีในทุกรูปแบบ นอกจากนี้ ควรมีการทดสอบความปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการจัดเก็บข้อมูลชีวมิติอย่างสม่ำเสมอ

## 6.2 มาตรฐานการบันทึกข้อมูลชีวมิติ

การบันทึกข้อมูลชีวมิติเพื่อใช้งานต่าง ๆ มีความจำเป็นและมีความสำคัญมาก ตามความจำเป็นดังที่กล่าวมาในหัวข้อ 5.3 ผู้ให้บริการต้องบันทึกข้อมูลอ้างอิงชีวมิติไว้ในฐานข้อมูลที่มีการรักษาความปลอดภัยสูงสุด ต้องไม่เก็บข้อมูลอ้างอิงชีวมิติรวมกับการเก็บเทมเพลตชีวมิติ หรือ รวมกับข้อมูลอัตลักษณ์ส่วนบุคคลของผู้ใช้บริการนั้น หรือใช้ชื่อไฟล์ที่เกี่ยวข้องกับข้อมูลอัตลักษณ์ส่วนบุคคลที่ทำให้สามารถชี้นำกลับไปถึงบุคคลเจ้าของข้อมูล เพื่อป้องกันข้อมูลรั่วไหลและย้อนกลับมาละเมิดสิทธิส่วนบุคคลของผู้ใช้บริการได้ การเก็บข้อมูลอ้างอิงชีวมิติต้องเก็บไว้ในฐานข้อมูลที่มีการป้องกันรักษาความปลอดภัยสูงสุดและถูกเข้าถึงและถูกใช้งานอย่างจำกัดเท่านั้น เนื่องจากถ้าข้อมูลอ้างอิงชีวมิติเหล่านี้หลุดรอดออกไปอยู่ในมือของอาชญากร บุคคลเจ้าของข้อมูลชีวมิติเหล่านี้ไม่สามารถเปลี่ยนลักษณะเฉพาะชีวมิติของตนเองได้

การบันทึกข้อมูลชีวมิติในรูปแบบสากลมีความจำเป็นสำหรับการใช้ข้อมูลชีวมิติและการแลกเปลี่ยนข้อมูลชีวมิติ โดยหน่วยงานที่ต้องพิสูจน์ยืนยันตัวตน ต้องบันทึกข้อมูลอ้างอิงชีวมิติตามมาตรฐานและแนวปฏิบัติดังต่อไปนี้

(1) การบันทึกข้อมูลชีวมิติ ต้องบันทึกข้อมูลอ้างอิงชีวมิติตาม *รูปแบบการแลกเปลี่ยนข้อมูลชีวมิติต่อขยายได้* (extensible biometric data interchange format) โดยกำหนดตามกรอบมาตรฐาน ISO/IEC 39794-1:2019 [12] และมีกรอบมาตรฐานเฉพาะสำหรับลักษณะเฉพาะชีวมิติบางประเภท ตัวอย่างเช่น

(1.1) การบันทึกข้อมูลภาพลายนิ้วมือ ต้องบันทึกข้อมูลตามมาตรฐาน ISO/IEC 39794-4:2019 [13]

(1.2) การบันทึกข้อมูลภาพใบหน้า ต้องบันทึกข้อมูลตามมาตรฐาน ISO/IEC 39794-5:2019 [14]

(1.3) การบันทึกข้อมูลภาพลายม่านตา ต้องบันทึกข้อมูลตามมาตรฐาน ISO/IEC 39794-6:2021 [15]

(1.4) การบันทึกข้อมูลภาพลายเส้นเลือด ต้องบันทึกข้อมูลตามมาตรฐาน ISO/IEC 39794-9:2021 [16]

(2) ในกรณีที่ข้อมูลชีวมิติประเภทนั้นยังไม่มีมาตรฐาน ISO/IEC 39794 ต้องบันทึกข้อมูลอ้างอิงชีวมิติตาม *รูปแบบการแลกเปลี่ยนข้อมูลชีวมิติ* (biometric data interchange format) โดยกำหนดตามกรอบมาตรฐาน ISO/IEC 19794-1:2011 [17] โดยเลือกใช้มาตรฐานการบันทึกชีวมิติเฉพาะประเภทในปีล่าสุด ตัวอย่างเช่น

(2.1) การบันทึกข้อมูลลายเซ็นลำดับเวลา (signature/sign time series data) ต้องบันทึกข้อมูลตามมาตรฐาน ISO/IEC 19794-7:2021 [18]

(2.2) การบันทึกข้อมูลเสียงพูด (voice data) ต้องบันทึกข้อมูลตามมาตรฐาน ISO/IEC 19794-13:2018 [19]

(2.3) การบันทึกข้อมูลดีเอ็นเอ (DNA data) ต้องบันทึกข้อมูลตามมาตรฐานใหม่คือ ISO/IEC 19794-14:202X [20] (มาตรฐานอยู่ในระหว่างการแก้ไข คาดว่าจะออกภายในปี 2022)

(3) ก่อนการบันทึก ข้อมูลตัวอย่างชีวมิติควรได้รับการประเมินคุณภาพก่อนการบันทึกข้อมูลอ้างอิงชีวมิติตามมาตรฐาน โดยค่าคุณภาพของข้อมูลตัวอย่างชีวมิติควรถูกเข้ารหัสข้อมูลและเก็บใน quality data field ตามรูปแบบการแลกเปลี่ยนข้อมูลชีวมิติ (biometric data interchange format) ซึ่งกำหนดตามมาตรฐาน ISO/IEC 29794-1;2016 [21]

(4) การบันทึกข้อมูลอ้างอิงชีวมิติ ต้องเก็บแยกในฐานข้อมูลอ้างอิงชีวมิติโดยเฉพาะ ซึ่งแยกกับเทมเพลตชีวมิติที่ใช้งานในระบบรู้จำชีวมิติอัตโนมัติและใช้ชื่อไฟล์ต้องเป็นชื่อที่ไม่เกี่ยวข้องกับข้อมูลอัตลักษณ์ของบุคคลเจ้าของชีวมิตินั้น เช่น เลขประจำตัวประชาชน ชื่อ นามสกุล การบันทึกข้อมูลอ้างอิงชีวมิติต้องเก็บในที่รักษาความลับและความปลอดภัยของข้อมูลสูงสุด การเชื่อมต่อกับเครือข่ายควรจำกัดและให้ความปลอดภัยสูงสุด การเข้าถึงข้อมูลอ้างอิงชีวมิติต้องเป็นในกรณีที่สำคัญและจำเป็นดังที่กล่าวไว้ ดังนั้น การเข้ารหัสไฟล์และการจำกัดจำนวนเจ้าหน้าที่ผู้สามารถเข้าถึงข้อมูลเหล่านี้ได้เป็นสิ่งที่จำเป็น แนวทางที่สามารถทำได้คือ การบันทึกข้อมูลการใช้งานชีวมิติแบบแคปซูลเวลา (time capsule) ซึ่งเน้นการบันทึกข้อมูลเกี่ยวข้องกับการยืนยันตัวตนที่ใช้ชีวมิติอย่างต่อเนื่องของแต่ละบุคคล โดยสามารถอ่านข้อมูลได้เพียงอย่างเดียวไม่ให้แก้ไขหรือลบข้อมูล โดยการอ่านข้อมูลอ้างอิงชีวมิติจากฐานข้อมูลนี้ให้ทำได้ในกรณีที่สำคัญและจำเป็นเท่านั้นดังกล่าวไว้แล้วในหัวข้อ 5.3 ในกรณีที่ผู้ใช้บริการยกเลิกบริการหรือเสียชีวิตจะเป็นกรณีเดียวที่สามารถลบข้อมูลอ้างอิงชีวมิติและข้อมูลที่เกี่ยวข้องทั้งหมดออกจากระบบได้

## 6.3 ข้อเสนอแนะการประเมินคุณภาพข้อมูลอ้างอิงชีวมิติ

คุณภาพข้อมูลตัวอย่างชีวมิติ (biometric sample quality) หมายถึง ค่าที่สะท้อนคุณภาพของข้อมูลตัวอย่างชีวมิติที่เก็บได้ ซึ่งควรจะมีลักษณะชีวมิติที่ชัดเจน มีความคมชัดเหมือนเหมือนต้นฉบับ และสามารถนำไปใช้กับระบบรู้จำชีวมิติอัตโนมัติได้อย่างมีประสิทธิภาพที่ดี ตามข้อกำหนดในมาตรฐาน ISO/IEC 29794-1;2016 [21]

การประเมินคุณภาพข้อมูลตัวอย่างชีวมิติมีความสำคัญต่อความน่าเชื่อถือและความแม่นยำของระบบ IdMS ข้อมูลตัวอย่างชีวมิติที่มีคุณภาพดี จะส่งผลให้ระบบรู้จำชีวมิติทำงานได้เต็มประสิทธิภาพและให้ผลลัพธ์ที่มีความแม่นยำสูง ข้อเสนอแนะสำหรับการประเมินคุณภาพข้อมูลตัวอย่างชีวมิติมีดังต่อไปนี้

(1) ค่าคุณภาพของข้อมูลตัวอย่างชีวมิติที่วัดได้ ต้องสะท้อนถึงการความแม่นยำของระบบ หมายถึง คุณภาพของข้อมูลตัวอย่างชีวมิติที่ดี จะทำให้การพิสูจน์ยืนยันตัวตน หรือการระบุตัวตนมีความแม่นยำสูง
(2) การประเมินคุณภาพข้อมูลตัวอย่างชีวมิติบางประเภท มีข้อเสนอแนะตามมาตรฐานดังต่อไปนี้
   (2.1) การวัดคุณภาพของชีวมิติประเภทลายนิ้วมือ มีข้อเสนอแนะตามมาตรฐาน ISO/IEC 29794-4;2017 [22]
   (2.2) การวัดคุณภาพของชีวมิติประเภทใบหน้า มีข้อเสนอแนะตามรายงานทางเทคนิค ISO/IEC TR 29794-5;2010 [23] หรือให้ใช้มาตรฐานล่าสุด ซึ่งกำลังพัฒนาและคาดว่าจะออกในปี ค.ศ. 2022-2023
   (2.3) การวัดคุณภาพของชีวมิติประเภทลายม่านตา มีข้อเสนอแนะตามมาตรฐาน ISO/IEC 29794-6;2015 [24]
(3) ข้อเสนอแนะนี้ไม่ได้กำหนดวิธีการหรืออัลกอริทึมในการประเมินค่าคุณภาพข้อมูลตัวอย่างชีวมิติ แต่กำหนดให้ประเมินก่อนบันทึกเก็บข้อมูล ทำให้สามารถตรวจสอบคุณภาพของข้อมูลตัวอย่างชีวมิติได้ภายหลัง
(4) ในกรณีที่ค่าคุณภาพข้อมูลตัวอย่างชีวมิติต่ำ สามารถดำเนินการเก็บข้อมูลตัวอย่างชีวมิติซ้ำเพื่อที่จะได้ตัวอย่างที่มีคุณภาพที่ดีกว่า แต่ในกรณีที่ซ้ำแล้วยังมีคุณภาพต่ำเหมือนเดิม ต้องหาสาเหตุเพื่อยกเว้นการเก็บตัวอย่าง หรือเก็บตัวอย่างที่มีคุณภาพต่ำไว้เพื่อประเมินและหาทางแก้ไขในอนาคต

## 6.4 มาตรฐานการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน

การแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน มีความต้องการและมีความจำเป็นในบางกรณี เช่นการนำข้อมูลมารวมกันเพื่อจัดตั้งหน่วยงานที่มีหน้าที่ใหม่ แต่เนื่องจากมีกรอบกฎหมายที่ไม่สามารถแลกเปลี่ยนข้อมูลได้อย่างอิสระ เช่น พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 [25] และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [10] ทำให้การแลกเปลี่ยนข้อมูลชีวมิติเป็นเรื่องที่ต้องให้ความระมัดระวังและมีความรอบคอบอย่างสูงสุดและอยู่ภายใต้กฎหมายทั้งสองฉบับนี้ ปัจจุบันการแลกเปลี่ยนข้อมูลชีวมิติอยู่ในวงจำกัดและไม่ได้มีการกำหนดให้ใช้มาตรฐานใด

ในกรณีที่จะมีการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน ควรอยู่ในรูปแบบมาตรฐานสากล คือ รูปแบบการแลกเปลี่ยนชีวมิติร่วมกัน (common biometric exchange formats: CBEF) ซึ่งกำหนดอยู่ในมาตรฐาน ISO/IEC 19785-1:2020 [26] การแลกเปลี่ยนข้อมูลต้องผ่านช่องทางที่มีความปลอดภัย เมื่อมีการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน ข้อมูลตัวอย่างชีวมิติต้องถูกเข้ารหัส และข้อมูลที่เข้ารหัสแล้วต้อง

แยกส่วนกับข้อมูลส่วนบุคคลอื่น ๆ โดยส่งข้อมูลเหล่านี้แยกกันไม่รวมกัน เพื่อป้องกันข้อมูลตัวอย่างชีวมิติในกรณีที่ข้อมูลอยู่ในระหว่างนำส่งโดยเจ้าหน้าที่ผู้ประสานงานหรือในกรณีที่มีการดักจับข้อมูลระหว่างหน่วยงาน เจ้าหน้าที่ผู้รับผิดชอบจะเข้าถึงข้อมูลส่วนนี้ได้จะต้องได้รับกุญแจในการถอดรหัสในช่องทางที่มีการรักษาความปลอดภัยข้อมูลสูงสุด

## 6.5 แนวทางการจัดการข้อมูลชีวมิติและข้อมูลอื่น

ในการบริหารจัดการอัตลักษณ์บุคคล ข้อมูลชีวมิติจะมีการเชื่อมต่อกับข้อมูลอัตลักษณ์ และข้อมูลเกี่ยวข้องกับบุคคล ซึ่งข้อมูลบุคคลอาจมาได้จากหลายแหล่งไม่ว่าจะเป็นจากภาครัฐหรือภาคเอกชน จำเป็นต้องมีแนวทางของการยืนยันข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่ต้องมีความน่าเชื่อถือได้

### 6.5.1 การรวมกันของข้อมูลชีวมิติ

องค์กรควรพิจารณาการนำข้อมูลชีวมิติ ซึ่งอาจเป็นประเภทอื่นจากหน่วยงานอื่น มารวมกัน ทำให้เพิ่มศักยภาพของการทำงาน ข้อมูลอัตลักษณ์จากหน่วยงานต่าง ๆ จะต้องถูกตรวจสอบความถูกต้องและความน่าเชื่อถือได้

เมื่อมีการรวมสองฐานข้อมูลเข้าด้วยกัน แต่ละฐานข้อมูลมีข้อมูลของแต่ละบุคคล มีความจำเป็นที่ต้องสร้างความมั่นใจในการนำข้อมูลของบุคคลคนเดียวกันมารวมกัน ทั้งนี้ทำได้ก็ต่อเมื่อสามารถยืนยันตัวตนได้อย่างถูกต้องว่าเป็นคนคนเดียวกันจากฐานข้อมูลทั้งสองฐาน ระเบียนทั้งสองจึงจะนำมารวมกันได้ ในขณะเดียวกันที่ต้องมั่นใจว่า ข้อมูลจากคนสองคนที่แตกต่างกันจะไม่ถูกนำมารวมกันเป็นระเบียนของคนเดียวกัน ซึ่งในกรณีเหล่านี้จะเกิดขึ้นได้ถ้าทั้งสองฐานข้อมูลมีเขตข้อมูล (field) ร่วมกันในจำนวนที่น้อยมาก อีกทั้งข้อมูลในเขตข้อมูลเหล่านี้มีความเหมือนและเป็นเอกลักษณ์ ตัวอย่างเช่นสองฐานข้อมูลใช้ลักษณะเฉพาะชีวมิติที่เหมือนกัน เช่น ใช้ลายนิ้วมือนิ้วเดียวกัน หรือใช้ม่านตาข้างเดียวกัน จะทำให้มีแนวโน้มที่สามารถจะนำข้อมูลมารวมกันในอนาคตอันใกล้ ด้วยการนำข้อมูลอ้างอิงชีวมิติมาเข้าคู่กันเพื่อตรวจสอบว่ามาจากบุคคล ๆ เดียวกันหรือไม่

เมื่อสองฐานข้อมูลเข้ามารวมกันโดยมีข้อมูลอ้างอิงชีวมิติแบบเดียวกัน แต่ไม่ได้มีการตรวจสอบเปรียบเทียบจริง ต้องติดป้ายระบุ (tag) กับข้อมูลเหล่านี้ เพื่อให้สามารถแยกระเบียนเหล่านี้ออกจากกันได้ในอนาคต ทำให้สามารถตรวจสอบข้อมูลได้ในกรณีที่มีความผิดพลาดในการนำระเบียนข้อมูลของต่างบุคคลมารวมกัน

การรวมฐานข้อมูลเข้าด้วยกันโดยจะเก็บรวบรวมข้อมูลอัตลักษณ์บุคคลที่ติดมาด้วย อาจเกิดปัญหาการละเมิดสิทธิส่วนบุคคลได้ [10] การจะใช้ลักษณะเฉพาะชีวมิติในการระบุตัวตนและรวมระเบียนเข้าด้วยกันอาจเกิดปัญหาเกี่ยวข้องกับข้อมูลส่วนบุคคลและความปลอดภัยของข้อมูลได้ ตัวอย่างในกรณีที่บุคคลสามารถมีอัตลักษณ์ได้หลายอัตลักษณ์โดยถูกกฎหมาย เช่น กรณีการคุ้มครองพยาน ที่ต้องสร้างอัตลักษณ์ใหม่ให้กับพยาน

การนำข้อมูลมารวมกันควรพิจารณาคุณค่าของการนำข้อมูลมารวมกัน ซึ่งสามารถพิจารณาได้จากความน่าเชื่อถือของข้อมูลซึ่งขึ้นอยู่กับหน่วยงานต้นทางและความซื่อสัตย์ในกระบวนการลงทะเบียน

### 6.5.2 การจัดการข้อมูล

องค์กรควรกำหนดนโยบายการจัดการข้อมูลชีวมิติ ระดับการเข้าถึงข้อมูลชีวมิติ รวมถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้ชัดเจน โดยถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและเกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล [10]

(1) **การจำกัดการเข้าถึงข้อมูล** ในบางกรณีที่ข้อมูลอาจถูกจำกัดหรือถูกระงับเนื่องจากผู้ใช้หรือผู้ควบคุมถูกจำกัดการเข้าถึงข้อมูล แต่ข้อมูลจริงยังคงอยู่ในระบบรู้จำชีวมิติอัตโนมัติและสามารถนำไปเข้าคู่ได้อย่างต่อเนื่อง ตัวอย่างเช่น ระบบรู้จำใบหน้า อาจปกปิดหรือแทนที่ภาพใบหน้าจริงที่เข้าคู่ได้ด้วยไอคอนหรือสัญลักษณ์ แต่เมื่อต้องตรวจเปรียบเทียบแบบเทียบเคียงสามารถแสดงอัตราการเข้าคู่และตำแหน่งเพื่อใช้ในการตัดสินใจ ในกรณีที่ไม่สามารถดูภาพจริงได้

(2) **การลบข้อมูลทิ้ง** องค์กรควรกำหนดนโยบายการลบข้อมูลชีวมิติตามขอบเขตอำนาจหรือตามกฎหมาย ซึ่งข้อมูลชีวมิติถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและได้รับการคุ้มครองจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล [10]

(3) **การเปลี่ยนแปลงข้อมูล** การเปลี่ยนข้อมูลในอัตลักษณ์ของบุคคลสามารถกระทำได้ เช่น การเปลี่ยนแปลงชื่อ-นามสกุล ดังนั้น ข้อมูลชีวมิติต้องใช้เลขที่อ้างอิงของตัวระบุอ้างอิงชีวมิติที่ไม่ซ้ำกันเป็นหลัก และไม่ควรเชื่อมโยงกับชื่อ-นามสกุล หรือแม้แต่เลขประจำตัวประชาชน ซึ่งทำให้เมื่อบุคคลทำการเปลี่ยนแปลงชื่อ-นามสกุล จึงไม่ต้องแก้ไขตัวเลขที่อ้างอิงของตัวระบุอ้างอิงชีวมิติ

(4) **การเปลี่ยนแปลงเงื่อนไข** ข้อมูลบางประเภทของอัตลักษณ์จะมีการใช้ค้นหาตัวตนควบคู่กันกับข้อมูลชีวมิติ เช่น ช่วงอายุ เพศ ดังนั้น องค์กรต้องกำหนดนโยบายของตนเองในการจัดการเปลี่ยนแปลงข้อมูลเพื่อป้องกันการแอบอ้างข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต ยกตัวอย่างเช่น เมื่อผู้ใช้เปลี่ยนเพศสภาพ ผู้ดูแลระบบควรมีกระบวนการและขั้นตอนการดำเนินการตรวจสอบที่รัดกุม

(5) **การเปลี่ยนแปลงข้อมูลชีวมิติ** ปกติใบหน้าจะเปลี่ยนแปลงไปตามเวลา รวมถึงการศัลยกรรมและการผ่าตัดเปลี่ยนแปลง ทำให้ข้อมูลชีวมิติที่ลงทะเบียนไว้แตกต่างจากข้อมูลชีวมิติในปัจจุบัน ดังนั้น องค์กรต้องกำหนดนโยบายในการจัดการเปลี่ยนแปลงข้อมูลชีวมิติ โดยใช้เลขที่อ้างอิงเดิมของตัวระบุอ้างอิงชีวมิติ ทั้งนี้ หากผู้ใช้ประสบปัญหาการเข้าใช้งานอยู่บ่อยครั้ง การเปลี่ยนแปลงข้อมูลชีวมิติสามารถช่วยลดความผิดพลาดในการถูกปฏิเสธตัวตนของระบบ IdMS ได้ แต่ต้องถูกตรวจสอบถึงสาเหตุการเปลี่ยนแปลง เพื่อมิให้ถูกสวมตัว หรือเปลี่ยนแปลงเพื่อกระทำทุจริต

(6) **การปลอมข้อมูลชีวมิติ** การใช้งานชีวมิติอาจมีความเสี่ยงต่อการโจมตีด้วยการปลอมแปลง ดังนั้น องค์กรต้องมีมาตรการรับมือที่มีประสิทธิภาพ และต้องมีระบบตรวจจับการโจมตีหลอกในระบบ IdMS นอกจากนี้องค์กรควรมีการทดสอบประสิทธิภาพของระบบการโจมตีอยู่เป็นประจำเพื่อให้มีความน่าเชื่อถือและมีความสมบูรณ์ในการใช้งาน ซึ่งระบบตรวจจับการโจมตีหลอกเป็นระบบที่มีวงจรชีวิตที่จำกัด เนื่องจากความซับซ้อนของการโจมตีที่ผู้ไม่หวังดีพัฒนาวิธีการเพิ่มขึ้นอย่างต่อเนื่อง ดังนั้นระบบตรวจจับการโจมตีหลอกจะต้องถูกพัฒนาอย่างต่อเนื่องเช่นกัน

(7) **การใช้อัตลักษณ์อื่นโดยถูกกฎหมาย** ในบางสถานการณ์ของการใช้งานข้อมูลชีวมิติอาจมีการร้องขอจากทางภาครัฐภายใต้กฎหมายที่เกี่ยวข้องเพื่อให้มีการเปลี่ยนหรือเพิ่มอัตลักษณ์ กับข้อมูลชีวมิติเดิมที่มีอยู่ในระบบ IdMS ซึ่งเป็นการสร้างตัวตนสมมติขึ้น ยกตัวอย่างเช่น โครงการคุ้มครองพยาน ดังนั้นในกรณีตัวอย่างนี้อาจทำให้มีข้อมูลอัตลักษณ์ของบุคคลสองชุดซึ่งใช้ข้อมูลชีวมิติร่วมกันสามารถเกิดขึ้นได้ในระบบได้ ดังนั้นต้องออกแบบระบบไว้รองรับกรณีเหล่านี้ด้วย

(8) **การใช้โทเค็นกับระบบรู้จำชีวมิติอัตโนมัติ** เมื่อนำความสามารถของระบบรู้จำชีวมิติอัตโนมัติมาใช้ในระบบที่ขึ้นอยู่กับการใช้โทเค็น เช่น บัตร รหัสผ่าน หรือ เลขรหัสอัตลักษณ์บุคคล (PIN) จะมีผลกระทบที่

สามารถเปิดเผยการปฏิบัติการต่าง ๆ โดยมิชอบ เช่น การลงทะเบียนหลายครั้งเพื่อให้ได้มาซึ่งโทเค็นหรือรหัสผ่านหลายอันเพื่อใช้ในทางที่มิชอบ (ตัวอย่างเช่น ใบขับขี่ต่างมลรัฐ) หรือ การใช้โทเค็นเพียงอันเดียวกับหลายบุคคล (ตัวอย่างเช่น บัตรผ่านรายปีเพื่อเข้าสถานที่ต่าง ๆ เช่น สวนสนุกดิสนีย์) เมื่อการใช้ในทางที่มิชอบได้ถูกเปิดเผย กระบวนการต่าง ๆ จะต้องทำให้ถูกต้องในการเก็บข้อมูลในอดีต โดยเฉพาะประเด็นที่มีผลกระทบเกี่ยวกับทางการเงิน

## 6.6 ข้อยกเว้นอื่น ๆ

องค์กรควรออกแบบการใช้เทคโนโลยีชีวมิติให้สามารถใช้ยืนยันตัวตน รวมถึงการตรวจจับการยืนยันตัวตนที่ใช้อัตลักษณ์ปลอมได้ เช่น บุคคลที่เปลี่ยนภาพใบหน้าบนบัตรประชาชน ใบขับขี่ หรือเอกสารทางการอื่น ๆ

ในกรณีที่บุคคลพิการ ขาดอวัยวะที่เกี่ยวข้องโดยตรงกับลักษณะเฉพาะชีวมิตินั้น ๆ เช่น ในกรณีที่ไม่มีดวงตาหรือตาบอด ไม่สามารถใช้ลายม่านตาในการพิสูจน์ยืนยันตัวตนได้ หรือ ในกรณีที่มือหรือแขนขาดไม่สามารถใช้ลายนิ้วมือในการพิสูจน์ยืนยันตัวตนได้ องค์กรควรมีข้อยกเว้น หรือใช้ชีวมิติหลายประเภทที่ผู้พิการสามารถใช้ทดแทนกันได้ หรือควรมีข้อแนะนำให้ใช้วิธีการอื่นที่มีประสิทธิภาพเท่าเทียมหรือสามารถทดแทนกันได้ในการยืนยันตัวตนสำหรับกลุ่มบุคคลผู้พิการ

องค์กรควรระมัดระวังการใช้ข้อมูลชีวมิติกับเด็ก หรืออาจยกเว้นการใช้งานชีวมิติกับเด็ก เนื่องจากความไม่เสถียรของชีวมิติที่มีการเปลี่ยนแปลงเนื่องจากการเจริญเติบโต ดังที่กล่าวมาแล้วในหัวข้อที่ 5.1 (4) การใช้งานชีวมิติในเด็กทำให้ระบบรู้จำชีวมิติเกิดความผิดพลาดสูง [8] โดยไม่ควรใช้ชีวมิติประเภทใบหน้ากับเด็กอายุต่ำกว่า 5 ปีเนื่องจากผลการรู้จำไม่น่าเชื่อถือ ต้องมีอายุตั้งแต่ 13 ปีการรู้จำใบหน้าจึงจะมีความเสถียร สำหรับชีวมิติประเภทลายนิ้วมือ แม้ว่าลายนิ้วมือจะมีเสถียรภาพตั้งแต่แรกเกิด แต่เซนเซอร์ต้องมีขนาดเล็กและมีความละเอียดภาพสูงมากกว่าปกติอย่างน้อยสองเท่าหรือมากกว่า 1,000 จุดต่อนิ้ว (dot per inch: dpi) นอกจากนี้อัลกอริทึมของระบบรู้จำลายนิ้วมืออัตโนมัติในอดีตไม่สามารถยืนยันตัวตนลายนิ้วมือของเด็กที่โตขึ้นเป็นผู้ใหญ่ได้ ปัญหานี้ได้มีการทดสอบในประเทศไทยตามรายงานวิจัย [27] ทำให้ยังไม่มีข้อสรุปในการกำหนดอายุขั้นต่ำในการใช้ลายนิ้วมือ [8] แต่สามารถอนุมาณได้ว่าสามารถใช้ได้ตั้งแต่วัยรุ่นหรืออายุมากกว่า 15 ปีเป็นต้นไป สำหรับชีวมิติประเภทลายม่านตาจะมีความเสถียรและสามารถใช้กับระบบรู้จำม่านตาอัตโนมัติตั้งแต่อายุ 8 ปี ขึ้นไป [8]

องค์กรควรระมัดระวังการใช้ข้อมูลชีวมิติกับเด็ก เนื่องจากการใช้เทคโนโลยีชีวมิติกับเด็กหรือผู้ที่ยังไม่บรรลุนิติภาวะ ตามมาตรา 20 กฎหมายคุ้มครองข้อมูลส่วนบุคคล กล่าวว่า “ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ดำเนินการ ดังต่อไปนี้

(1) ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

(2) ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

ตัวอย่างการใช้ชีวมิติกับเด็ก คือ การใช้เพื่อระบุตัวตนและป้องกันการสลับตัวเด็กแรกเกิด การใช้เพื่อระบุตัวเด็กที่ถูกลักพาตัวหรือการค้นหาเด็กที่สูญหาย การใช้ในโรงเรียน เช่น การลงทะเบียน การเช็คชื่อเข้าเรียน การยืมหนังสือห้องสมุด การใช้แทนเงินในโรงอาหาร เนื่องจากหลายประเทศมีกฎหมายคุ้มครองการเก็บข้อมูลชีวมิติของเด็ก การใช้งานชีวมิติต้องพิจารณาความเหมาะสมและความจำเป็นในการใช้งานชีวมิติกับเด็กซึ่งเป็นเรื่องละเอียดอ่อน นอกจากนี้ยังต้องได้รับความยินยอมจากพ่อ แม่ หรือผู้ปกครองตามกฎหมายอีกด้วย

องค์กรควรออกแบบการใช้เทคโนโลยีชีวมิติ ให้สามารถใช้พิสูจน์และยืนยันตัวตนบุคคลที่เป็นโรคอัลไซเมอร์หรือมีอาการหลงลืม รวมทั้งเด็กกำพร้าและเด็กไร้สัญชาติได้

การใช้เทคโนโลยีชีวมิติสำหรับผู้อพยพหรือแรงงานต่างด้าว สามารถใช้พิสูจน์และยืนยันตัวตน แต่ไม่สามารถใช้สืบประวัติหรือค้นหาข้อมูลได้ เนื่องจากข้อมูลอัตลักษณ์เดิมจากประเทศหรือเขตอำนาจศาลต้นทางไม่ปรากฏ หลายหน่วยงานอาจเก็บข้อมูลชีวมิติของบุคคลเหล่านี้โดยไม่สามารถเชื่อมต่อระหว่างหน่วยงาน ถ้าสามารถเชื่อมต่อข้อมูลอัตลักษณ์เหล่านี้เข้าด้วยกันได้ จะสามารถสร้างประวัติการทำงานหรือสุขภาพ ที่สามารถทำให้บุคคลเหล่านี้ สามารถดำรงชีวิตอยู่ภายใต้กฎหมายไทยได้โดยมีมาตรฐานเดียวกัน

## 7. ข้อเสนอแนะเกี่ยวกับการรักษาความปลอดภัยข้อมูลชีวมิติกับระบบบริหารอัตลักษณ์บุคคล

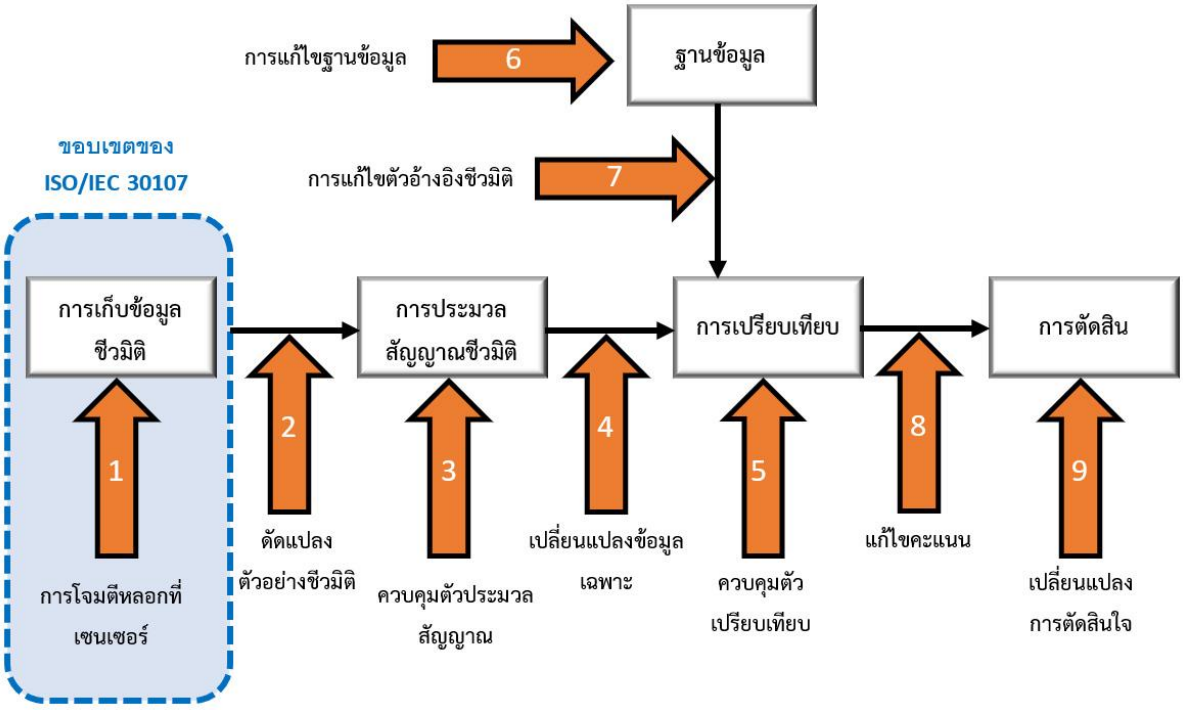
ข้อเสนอแนะในบทนี้ จะเน้นการรักษาความปลอดภัยของข้อมูลชีวมิติสำหรับระบบบริหารอัตลักษณ์บุคคล แต่ไม่ได้เกี่ยวข้องกับการรักษาความปลอดภัยของระบบบริหารอัตลักษณ์บุคคล

องค์กรที่ดูแลระบบ IdMS ต้องให้ความสำคัญโดยการรักษาความปลอดภัยในการเก็บข้อมูลอ้างอิงชีวมิติของแต่ละบุคคลในระดับสูงสุด เนื่องจากถ้าข้อมูลชีวมิติเหล่านี้ถูกนำออกไปใช้ในทางที่ผิดหรือถูกนำไปเผยแพร่ บุคคลที่ถูกนำข้อมูลชีวมิติไปใช้ไม่สามารถที่จะเปลี่ยนแปลงแก้ไขข้อมูลชีวมิติของตนได้

การรักษาความปลอดภัยของข้อมูลชีวมิติ มีประเด็นที่ต้องให้ความสำคัญอยู่สองประเด็น คือการป้องกันการโจมตีหลอก (presentation attack protection: PAP) และการป้องกันเทมเพลตชีวมิติ (biometric template protection) โดยมีรายละเอียดดังต่อไปนี้

### 7.1 การป้องกันการโจมตีหลอก

มาตรฐาน ISO/IEC 30107-1:2016 [28] ได้กำหนดขอบเขตการโจมตีระบบรู้จำชีวมิติอัตโนมัติ ซึ่งสามารถโจมตีระบบได้จากที่ใดก็ได้และสามารถเป็นบุคคลใดก็ได้ ดังแสดงในรูปที่ 4 โดยมาตรฐานนี้จะเกี่ยวข้องกับการโจมตีที่เซนเซอร์หรือตัวรับข้อมูลชีวมิติเท่านั้น ซึ่งแสดงในกรอบเส้นประตามรูปที่ 4 เท่านั้น เนื่องจากส่วนอื่นเป็นการโจมตีที่ต้องอยู่ในระบบรู้จำชีวมิติอัตโนมัติทั้งหมด




**รูปที่ 4 แสดงผังความเป็นไปได้ในการโจมตีระบบรู้จำชีวมิติอัตโนมัติในขั้นตอนต่าง ๆ** [28]

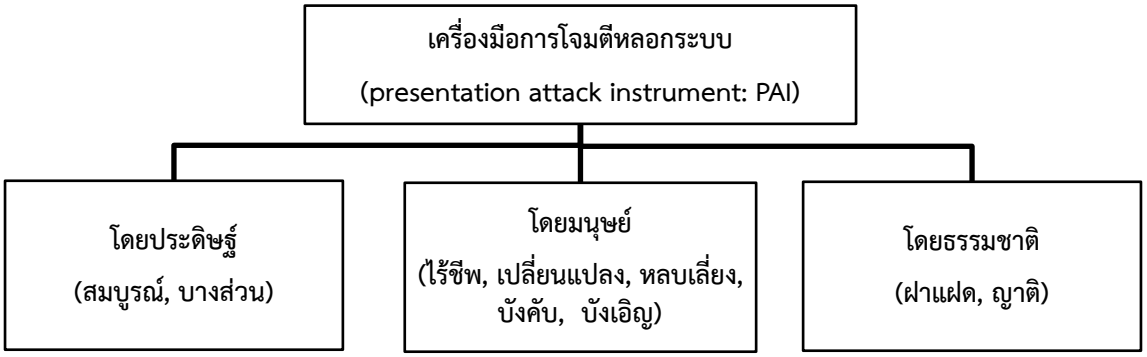
มาตรฐาน ISO/IEC 30107-1:2016 [28] ได้กำหนดการโจมตีระบบรู้จำชีวมิติอัตโนมัติ ซึ่งเกิดจากบุคคลสองประเภท คือ ผู้ปลอมตัวตน (biometric imposter) และผู้ปกปิดตัวตน (biometric concealer)

ผู้ปลอมตัวตน คือ ผู้ต้องการหลอกระบบว่าตนเองเป็นบุคคลที่ระบบให้การยืนยันตัวตน โดยผู้ปลอมตัวตนสามารถหลอกระบบได้สองแนวทาง คือ หลอกว่าเป็นบุคคลบุคคลหนึ่งโดยเฉพาะเจาะจง หรือ หลอกว่าเป็นบุคคลใดก็ได้ที่อยู่ในฐานข้อมูลที่สามารถเข้าถึงได้ โดยไม่มีข้อมูลเฉพาะเจาะจงกับบุคคลใดบุคคลหนึ่ง

ผู้ปกปิดตัวตน คือ ผู้ต้องการหลอกระบบว่าตนเองไม่ใช่เป็นบุคคลที่ระบบให้การยืนยันตัวตน โดยการเปลี่ยนแปลง ดัดแปลง ปกปิด เพิ่มเติมลักษณะเฉพาะชีวมิติให้แตกต่างจากเดิม ทำให้ระบบไม่สามารถรู้จำบุคคลเดิมที่มีอยู่ในฐานข้อมูลได้ การโจมตีแบบปกปิดตัวตนมีได้สองแนวทาง คือ โจมตีเพื่อหาแนวทางการหลอกชีวมิติหรือเปลี่ยนแปลงชีวมิติในภายหลัง กับโจมตีเพื่อใช้เพียงครั้งเดียว

### 7.1.1 เครื่องมือการโจมตีหลอกระบบ (PAI)

มาตรฐาน ISO/IEC 30107-1:2016 [28] ได้กำหนดตัวอย่างการปลอมชีวมิติจะถูกแบ่งหมวดหมู่ตามประเภทต่าง ๆ ซึ่งจะเรียกว่า เครื่องมือการโจมตีหลอกระบบ (presentation attack instrument: PAI) โดยสามารถจำแนกประเภทได้ดังรูปที่ 5




**รูปที่ 5 การจำแนกประเภทเครื่องมือการโจมตีหลอกระบบ**

มาตรฐาน ISO/IEC 30107-1:2016 [28] จะแบ่งเครื่องมือการโจมตีหลอกระบบได้เป็นสามประเภท ตามรูปที่ 5 โดยมีรายละเอียดดังต่อไปนี้

**(1) เครื่องมือการโจมตีหลอกโดยการประดิษฐ์ (artificial)** เครื่องมือการโจมตีหลอกระบบประเภทนี้ เป็นการประดิษฐ์ขึ้นเพื่อหลอกระบบ โดยสามารถแบ่งย่อยเป็น

**(1.1) สมบูรณ์ (complete)** เป็นการประดิษฐ์ขึ้นอย่างสมบูรณ์ทั้งหมด เช่น การปลอมนิ้วมือจากยาง ทั้งนิ้ว การปลอมลูกตารวมทั้งลายม่านตาทั้งชิ้น การใช้วีดิทัศน์ของใบหน้าหลอกระบบ

**(1.2) บางส่วน (partial)** เป็นการประดิษฐ์ขึ้นเพียงบางส่วน เช่น ผิววัสดุเทียมลายนิ้วมือแปะติดกับนิ้วจริง คอนแทคเลนส์ปลอมลายม่านตา แว่นตากันแดด หรือการแต่งหน้าที่ทำให้ไม่เหมือนตัวเอง

**(2) เครื่องมือการโจมตีหลอกโดยมนุษย์ (human)** เครื่องมือการโจมตีหลอกระบบประเภทนี้ มนุษย์จะคิดค้นขึ้นและหาวิธีต่าง ๆเพื่อหลอกระบบ โดยสามารถแบ่งย่อยเป็น

**(2.1) ไร้ชีพ (lifeless)** เช่น ชิ้นส่วนซากศพ นิ้วมือขาด หรือ มือขาด

**(2.2) เปลี่ยนแปลง (altered)** เช่น ทำให้เสียโฉม ศัลยกรรม ผ่าตัดเปลี่ยนรอยนิ้วมือหรือนิ้วเท้า

**(2.3) หลบเลี่ยง (non-conformant)** เช่น การแสดงสีหน้าให้แตกต่างไปด้วยอารมณ์ที่ไม่ใช่ปกติ เช่น หน้ายิ้ม หรือหน้าบึ้งมากกว่าปกติ การใช้ข้างนิ้วหรือปลายนิ้วสำหรับลายนิ้วมือ

**(2.4) บังคับ (coerced)** เช่น ในขณะที่บุคคลเจ้าของชีวมิติหมดสติ หรือ ถูกบังคับขู่เข็ญให้ใช้ชีวมิติของตน

**(2.5) บังเอิญ (conformant)** เช่น การปลอมแปลงแบบไม่ต้องใช้ความพยายาม (zero effort impostor attempt) คือสามารถใช้ได้เนื่องจากลักษณะเฉพาะชีวมิติมีความเหมือนกัน

**(3) เครื่องมือการโจมตีหลอกโดยธรรมชาติ** เครื่องมือการโจมตีหลอกระบบประเภทนี้ เป็นโดยธรรมชาติ เช่น ฝาแฝดไข่ใบเดียวกันที่มีหน้าตาเหมือนกัน ใบหน้าที่มีความคล้ายกันโดยธรรมชาติ

### 7.1.2 การตรวจจับการโจมตีหลอกระบบ (PAD)

มาตรฐาน ISO/IEC 30107-1:2016 [28] ได้เสนอแนวทางการป้องกันการโจมตีหลอกระบบ (presentation attack detection: PAD) ซึ่งสามารถแบ่งได้เป็นสองแบบ คือ การตรวจจับการโจมตีหลอกผ่านการเก็บข้อมูลและการตรวจจับการโจมตีหลอกผ่านการเฝ้าระวังระบบ

**(1) การตรวจจับการโจมตีหลอกผ่านการเก็บข้อมูล (through data capture)** เป็นการตรวจจับการโจมตีหลอก ณ ส่วนที่รับข้อมูล เซนเซอร์ หรืออุปกรณ์เก็บข้อมูลตัวอย่างชีวมิติ ซึ่งเป็นการตรวจจับทางตรง การตรวจจับการโจมตีหลอกผ่านการเก็บข้อมูล มีได้หลายวิธีดังต่อไปนี้

**(1.1) การตรวจจับสิ่งแปลกปลอม (artefact detection)** เป็นการตรวจจับความผิดปกติของคุณสมบัติที่สามารถบ่งชี้ว่าเป็นสิ่งแปลกปลอม ตัวอย่างเช่น เซนเซอร์อ่านลายนิ้วมือที่สามารถวัดค่าความต้านทานต่อไฟฟ้ากระแสสลับ (impedance) ของผิวหนังที่มีค่าแตกต่างจากค่าของผิวหนังปกติ ซึ่งอาจหมายถึงการใช้วัสดุปลอมลายนิ้วมือแปะนิ้วไว้

**(1.2) การตรวจจับการมีชีวิต (liveness detection)** เป็นการตรวจจับคุณสมบัติต่าง ๆ ของการมีชีวิต ซึ่งอาจเป็นแบบธรรมชาติ เช่น เมื่อเปลี่ยนความสว่าง รูม่านตาจะปรับเปลี่ยนขนาดโดยอัตโนมัติ หรือ เป็นแบบควบคุม เช่น การสุ่มลำดับการสแกนนิ้วซึ่งผู้ใช้ต้องทำการสแกนนิ้วตามลำดับให้ถูกต้อง หรือ ตามคำสั่งให้หันใบหน้าไปทางที่กำหนด พยักหน้า หรือเอียงหน้า

**(1.3) การตรวจจับการเปลี่ยนแปลง (alteration detection)** เป็นการตรวจจับความผิดปกติที่เกิดจากการเปลี่ยนแปลง เช่น รอยแผลเป็นบนลายนิ้วมือที่เกิดขึ้นจากการพยายามเปลี่ยนแปลงลายนิ้วมือ การทำสีหน้าหรือแสดงอารมณ์ที่แตกต่างจากใบหน้าปกติ

**(1.4) การตรวจจับความไม่สอดคล้องกัน (non-conformance detection)** เป็นการตรวจจับความผิดปกติที่เกิดจากความไม่สอดคล้องกัน เช่น ระดับความเข้มของแสงไม่คงที่เมื่อเทียบกับสภาวะปกติ หรือในกรณีใช้สมาร์ทโฟนเก็บภาพชีวมิติ การควบคุมแสงสีจากหน้าจอสมาร์ทโฟนและวิเคราะห์แสงสะท้อนจากภาพชีวมิติว่าสอดคล้องกับแสงสีที่ส่งออกไปหรือไม่

**(1.5) การตรวจจับการบีบบังคับ (coercion detection)** เป็นการตรวจจับความผิดปกติที่เกิดจากถูกบีบบังคับ เช่น การวิเคราะห์ความเครียดจากโทนเสียงหรือเสียงผิดปกติจากสภาพแวดล้อม หรือการตรวจจับการแสดงอารมณ์บนใบหน้า

**(1.6) การตรวจจับการปกปิด (obscuration detection)** เป็นการตรวจจับความผิดปกติที่เกิดจากการถูกปกปิด หรือพยายามบดบัง เช่น อุปกรณ์หรือเครื่องแต่งกายที่ปกปิดบางส่วนของใบหน้า เช่น ผ้าพันคอหรือหมวก

**(2) การตรวจจับการโจมตีหลอกผ่านการเฝ้าระวังระบบ (through system monitoring)** การตรวจจับการโจมตีหลอกที่ผ่านการเฝ้าระวังระบบ เป็นการตรวจจับทางอ้อม มีได้หลายวิธีดังต่อไปนี้

(2.1) การนับจำนวนความพยายามที่ล้มเหลว (failed attempt detection counter) เป็นการตรวจจับความผิดปกติที่เกิดจากการพยายามเข้าระบบหลายครั้งและล้มเหลว สังเกตความพยายามในการเข้าระบบแล้วล้มเหลวเหมือน ๆ กันหลายครั้ง เพื่อใช้ในการตรวจจับเหตุการณ์ผิดปกติ การทุจริต รวมถึงใช้เป็นหลักฐานทางกฎหมาย ดังนั้นการเก็บบันทึกข้อมูลที่เกี่ยวข้องในการยืนยันตัวตนแต่ละครั้งในตลอดช่วงเวลาที่ผู้ใช้บริการอยู่ในการดูแลของผู้ให้บริการมีความจำเป็นอย่างยิ่ง ควรจัดเก็บในทุกกรณีไม่ว่าการยืนยันตัวตนจะประสบความสำเร็จหรือล้มเหลว รวมทั้งควรจัดเก็บข้อมูลที่เกี่ยวข้องให้ครอบคลุมเพียงพอรวมถึงข้อมูลชีวมิติที่ใช้ คะแนนความเหมือนที่ได้ โดยจัดเก็บข้อมูลเหล่านี้อย่างรัดกุมเชื่อถือได้และปลอดภัย

(2.2) การใช้ตำแหน่งและเวลาที่สอดคล้อง (geographic and temporal) เป็นการตรวจจับความผิดปกติที่เกิดจากตำแหน่งและเวลา ซึ่งบุคคลปกติจะมีพฤติกรรมการใช้งานระบบที่ตำแหน่งและเวลาที่สอดคล้องกัน เมื่อไรที่เกิดความผิดปกติไม่ว่าจะเป็นเวลา หรือตำแหน่งที่ใช้มีความขัดแย้งหรือแปลกแยกจากปกติวิสัย เป็นไปได้ว่าจะมีการโจมตีหลอก หรือถูกบีบบังคับให้กระทำ

(2.3) ระบบตรวจตราด้วยกล้องวงจรปิด (video surveillance) เป็นการใช้กล้องวงจรปิดเพื่อรักษาความปลอดภัย โดยใช้เป็นเครื่องมือในการป้องกันและตรวจจับความผิดปกติบริเวณที่เกิดจากการโจมตี

บุคคลที่โจมตีจะมีพฤติกรรมที่แตกต่างจากผู้ใช้ปกติ ทำให้ผู้ควบคุมหรือระบบวิเคราะห์วิดิทัศน์สามารถตรวจจับความผิดปกติหรือการโจมตีหลอกได้ ควรบันทึกข้อมูลวิดิทัศน์ไว้ตลอดการเข้าใช้งานของผู้ใช้บริการ ซึ่งสามารถจะใช้คลี่คลายปัญหาที่อาจเกิดขึ้นได้ในภายหลัง

## 7.2 การป้องกันเทมเพลตชีวมิติ

โดยปกติแล้ว เมื่อได้รับข้อมูลตัวอย่างชีวมิติ ระบบรู้จำชีวมิติอัตโนมัติจะทำการประมวลผลและสกัดเอาลักษณะสำคัญของข้อมูลตัวอย่างชีวมิติออกมาเก็บไว้ในรูปแบบเทมเพลตชีวมิติ (biometric template) เมื่อผู้ใช้บริการแสดงชีวมิติเพื่อการยืนยันตัวตน ระบบรู้จำชีวมิติอัตโนมัติจะทำการเปรียบเทียบเทมเพลตที่ได้จากข้อมูลตัวอย่างชีวมิติกับเทมเพลตที่ได้จากข้อมูลอ้างอิงชีวมิติในฐานข้อมูลในรูปแบบหนึ่งต่อหนึ่ง (one-to-one) การระบุตัวตนคือการเปรียบเทียบเทมเพลตที่ได้จากข้อมูลตัวอย่างชีวมิติของผู้ใช้บริการเปรียบเทียบกับเทมเพลตที่ได้จากข้อมูลอ้างอิงชีวมิติของบุคคลทั้งหมดในฐานข้อมูลในรูปแบบหนึ่งต่อกลุ่ม (one-to-many)

สังเกตุว่าข้อมูลตัวอย่างชีวมิติจะถูกใช้งานเฉพาะตอนถูกสกัดลักษณะสำคัญของข้อมูลชีวมิติเข้ามาอยู่ในรูปเทมเพลต ในกรณีที่จะต้องเก็บข้อมูลตัวอย่างชีวมิติเพื่อใช้งาน ผู้ให้บริการต้องเก็บและบันทึกข้อมูลตัวอย่างชีวมิติไว้ในฐานข้อมูลที่มีการรักษาความปลอดภัยสูงสุด ต้องไม่เก็บข้อมูลตัวอย่างชีวมิติรวมกับการเก็บเทมเพลต หรือ รวมกับข้อมูลอัตลักษณ์ส่วนบุคคลของผู้ใช้บริการนั้น เพื่อป้องกันข้อมูลรั่วไหลและย้อนกลับมาละเมิดสิทธิส่วนบุคคลของผู้ใช้บริการได้

โดยปกติ เทมเพลตชีวมิติจะเก็บในรูปแบบเฉพาะของแต่ละอัลกอริทึมการรู้จำชีวมิติอัตโนมัติ ซึ่งเป็นความลับของแต่ละบริษัทผู้ผลิตระบบรู้จำชีวมิติอัตโนมัติ ซึ่งอาจมีการเข้ารหัสเพื่อป้องกันความปลอดภัย หรืออยู่ในรูปแบบมาตรฐานเพื่อการแลกเปลี่ยนระหว่างระบบ เช่น เทมเพลตมาตรฐานของลายนิ้วมือ ISO/IEC 19794-2:2011 [29] ในกรณีที่เทมเพลตเก็บตามรูปแบบมาตรฐาน อาจมีโอกาสจะถูกนำไปสร้างกลับเป็นข้อมูลตัวอย่างชีวมิติได้ ซึ่งเป็นอันตรายต่อเจ้าของข้อมูลชีวมิติ เพื่อความปลอดภัยการจัดเก็บเทมเพลตควรแยกออกจากฐานข้อมูลส่วนบุคคลประเภทอื่น โดยไม่ระบุข้อมูลอ้างอิงที่สามารถระบุตัวตนของผู้ใช้บริการได้โดยตรง เช่น หมายเลขบัตรประชาชน ชื่อ นามสกุล สำหรับในกรณีที่เทมเพลตเก็บรูปแบบเฉพาะของแต่ละบริษัท อาจใช้งานได้เฉพาะระบบรู้จำชีวมิติอัตโนมัติที่ใช้ซอฟต์แวร์จากบริษัทเดียวกันเท่านั้น เมื่อนำไปใช้ต่างบริษัทจะไม่สามารถใช้งานได้ และโดยทั่วไปแล้วมีความปลอดภัยพอสมควรเนื่องจากเป็นความลับของทางบริษัท ไม่สามารถนำมาสร้างข้อมูลตัวอย่างชีวมิติกลับมาได้ยกเว้นแต่บริษัทผู้ผลิตให้ความร่วมมือ

มาตรฐาน ISO/IEC 30136:2018 [30] ได้อธิบายแนวทางการทดสอบเทมเพลตชีวมิติที่มีความปลอดภัย โดยเทมเพลตชีวมิติเหล่านี้จะมีคุณสมบัติคือ (1) จะไม่สามารถสร้างข้อมูลชีวมิติต้นฉบับย้อนกลับมาได้ (irreversibility) (2) สามารถสร้างเทมเพลตชีวมิติออกมาได้หลากหลายไม่ซ้ำกัน (diversity) และ (3) ไม่สามารถเชื่อมโยงกันเพื่อที่จะสร้างข้อมูลตัวอย่างชีวมิติย้อนกลับมาได้ (unlinkability) แต่ข้อเสียของเทมเพลตเหล่านี้คือประสิทธิภาพความแม่นยำของระบบรู้จำชีวมิติอัตโนมัติจะลดลงเนื่องจากเทมเพลตมีคุณสมบัติเหล่านี้ ทำให้ต้องใช้ข้อมูลลักษณะสำคัญเพียงบางส่วน ไม่ใช่ทั้งหมดเพื่อป้องกันการสร้างย้อนกลับ

ระบบที่มีการส่งเทมเพลทออกภายนอกหน่วยงาน ควรต้องมีระบบการป้องกันความปลอดภัยของข้อมูลตามมาตรฐาน ISO/IEC 30136:2018 [30]

## 8. ข้อเสนอแนะเกี่ยวกับสิทธิส่วนบุคคลกับข้อมูลชีวมิติ

สำหรับประเทศไทยมีกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่สำคัญอยู่สองฉบับคือ

(1) พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 [25]

(2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [10]

สำหรับ “ข้อมูลข่าวสารส่วนบุคคล” ในพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 [25] ได้ให้ความหมายความว่า “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น *ลายพิมพ์นิ้วมือ* แผ่นบันทึก *ลักษณะเสียงของคน*หรือ*รูปถ่าย* และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” จะเห็นได้ว่า ข้อมูลชีวมิติประเภทใบหน้า ลายนิ้วมือ และเสียงพูดได้ถูกกำหนดให้เป็น ข้อมูลข่าวสารส่วนบุคคล ในพระราชบัญญัติฉบับนี้ และได้รับความคุ้มครองโดยพระราชบัญญัติฉบับนี้ [25]

สำหรับ “ข้อมูลส่วนบุคคล” ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [10] ได้ให้ความหมายความว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” และได้กำหนดว่า “ข้อมูลชีวภาพ” หรือที่เรียกว่า “ชีวมิติ” ในมาตรฐานนี้เป็นข้อมูลส่วนบุคคล ซึ่งได้รับการคุ้มครองโดยพระราชบัญญัติฉบับนี้ [10]

เนื่องจากการใช้งานข้อมูลชีวมิติจะถูกตรวจสอบจากสังคมในเรื่องความเป็นส่วนตัวอย่างละเอียด การเก็บข้อมูลชีวมิติที่เชื่อมต่อกับข้อมูลอัตลักษณ์ที่เกี่ยวกับความเป็นส่วนตัวต้องให้ความสำคัญสูงสุด ซึ่งควรจะมีข้อจำกัดในการเก็บข้อมูลส่วนบุคคลและข้อมูลเหล่านี้ซึ่งต้องได้มาถูกต้องตามกฎหมาย รวมถึงบุคคลที่ถูกเก็บข้อมูลชีวมิติควรได้รับทราบหรือยินยอมก่อน

การยอมรับข้อเสนอเกี่ยวกับประเด็นสิทธิส่วนบุคคลในทางปฏิบัติในช่วงต้น ๆ ของการพัฒนาระบบจะช่วยลดแนวโน้มที่จะเกิดผลกระทบในเรื่องความเป็นส่วนตัว การประเมินผลกระทบสิทธิส่วนบุคคล (privacy impact assessment: PIA) ควรนำมาใช้เพื่อตัดสินใจเกี่ยวกับระบบและการเริ่มโครงการการเก็บข้อมูลใหม่ที่จะมีผลกระทบกับสิทธิส่วนบุคคลโดยตรง และความเป็นไปได้ในการมองเห็นการนำไปใช้อย่างผิดประเภท การนำไปใช้อย่างผิดประเภท โดยเอกสารเกี่ยวกับ PIA จะให้แนวทาง นโยบาย และ ความต้องการ ให้องค์กรยึดถือปฏิบัติในการจัดการข้อมูลที่สามารถอธิบายได้

คุณสมบัติของข้อมูลชีวมิติถูกจัดให้เป็นข้อมูลที่สามารถระบุตัวตนได้ (personally identifiable information: PII) ตัวอย่างเช่น ลายนิ้วมือและลายม่านตาสามารถเชื่อมโยงถึงแต่ละบุคคลได้ โดยหลักปฏิบัติสารสนเทศอย่างเท่าเทียม (fair information practice principles: FIPPS) ควรนำมาประยุกต์ใช้กับชีวมิติดังต่อไปนี้

**(1) ความโปร่งใส (transparency)** ออกคำเตือนให้กับแต่ละบุคคลเกี่ยวกับ การเก็บข้อมูล การใช้งาน การเปิดประเด็นเพื่อการถกเถียงและโต้แย้งอย่างกว้างขวาง และ การบำรุงรักษา ข้อมูลที่สามารถระบุตัวตนได้ (PII)

**(2) การมีส่วนร่วมของแต่ละบุคคล (individual participation)** เกี่ยวข้องกับแต่ละบุคคลในกระบวนการใช้ PII สู่ขอบเขตที่สามารถปฏิบัติได้ โดยหาทางให้บุคคลยอมรับการเก็บ การใช้ การเปิดประเด็นเพื่อการถกเถียงและโต้แย้งอย่างกว้างขวาง และการบำรุงรักษา PII นอกจากนี้ยังให้กลไกสำหรับการเข้าถึงอย่างเหมาะสม การทำให้ถูกต้อง และ การชดเชย เกี่ยวกับการที่องค์กรใช้ PII

(3) **ข้อกำหนดเป้าหมาย (purpose specification)** องค์กรควรสื่อสารอย่างชัดเจนโดยเฉพาะเป็นผู้ที่มีอำนาจซึ่งได้รับอนุญาตในการเก็บข้อมูล PII และ องค์กรควรสื่อสารอย่างชัดเจนโดยเฉพาะวัตถุประสงค์ในการนำ PII ไปใช้งาน

(4) **ข้อมูลน้อยที่สุด (data minimization)** องค์กรควรเก็บข้อมูล PII เพียงเพื่อใช้ในสิ่งที่เกี่ยวข้องและจำเป็นเพื่อที่จะบรรลุวัตถุประสงค์ที่กำหนดและจะเก็บข้อมูล PII ไว้นานเท่าที่จำเป็นเพื่อที่จะบรรลุวัตถุประสงค์เท่านั้น

(5) **ใช้อย่างจำกัด (use limitation)** องค์กรควรใช้ข้อมูล PII เพียงเพื่อวัตถุประสงค์ที่กำหนดในคำเตือนการให้ข้อมูล PII นอกองค์กรควรมีวัตถุประสงค์ที่เข้ากันได้กับวัตถุประสงค์ในการเก็บข้อมูล PII

(6) **คุณภาพของข้อมูลและความซื่อสัตย์ (data quality and integrity)** องค์กรควรทำให้แน่ใจว่า ข้อมูล PII มีความแม่นยำ เกี่ยวข้อง เหมาะสมกับเวลา และสมบูรณ์ ในขอบเขตที่สามารถปฏิบัติได้

(7) **ความมั่นคงปลอดภัย (security)** องค์กรควรป้องกันข้อมูล PII ในทุกรูปแบบโดยเครื่องป้องกันความปลอดภัยที่เหมาะสมต่อความเสี่ยงต่าง ๆ ได้แก่ การหาย การเข้าถึงหรือการใช้โดยไม่ได้รับอนุญาต การทำลาย การดัดแปลง หรือ การเปิดเผยโดยไม่ได้ตั้งใจหรือไม่เหมาะสม

(8) **ภาระความรับผิดชอบและการตรวจสอบภายใน (accountability and auditing)** องค์กรควรมีภาระความรับผิดชอบโดยทำตามกฎระเบียบ โดยจัดการอบรมให้เจ้าหน้าที่ผู้ปฏิบัติงานและผู้ทำสัญญาที่ใช้งาน PII รวมถึงการตรวจสอบภายในการใช้งาน PII โดยการสาธิตการปฏิบัติตามกฎระเบียบและข้อกำหนดในการป้องกันการละเมิดสิทธิส่วนบุคคลที่เป็นไปได้ทั้งหมด

การประยุกต์ใช้งานหลักปฏิบัติสารสนเทศอย่างเท่าเทียม (FIPPS) เพื่อลดผลกระทบที่เกี่ยวข้องและจัดการปัญหาหลักต่าง ๆ ที่เกิดขึ้น รวมทั้ง

(1) **ลักษณะเฉพาะคุณภาพต่ำ (poor quality characteristics)** เกิดจากการมีอายุมาก วิธีการเก็บ หรืออาชีพ (เช่น ลายนิ้วมือของ ช่างปูน หรือ ชาวประมง จะมีคุณภาพต่ำหรือไม่สามารถเก็บได้) ควรมีแนวทางการละเว้นสำหรับบุคคลที่ไม่มีชีวมิติ หรือมีชีวมิติที่มีคุณภาพต่ำ หรือผู้พิการ

(2) **การเก็บข้อมูลชีวมิติอย่างเปิดเผย (overt collection)** บุคคลควรรับรู้ว่าข้อมูลชีวมิติของเขาถูกเก็บการเก็บข้อมูลชีวมิติควรเป็นอย่างเปิดเผย

(3) **การวัดการป้องกันข้อมูลอย่างเข้มแข็ง (strong data protection measures)** การเข้ารหัสเมื่อเก็บข้อมูล หรือในช่วงการส่งผ่านข้อมูล ข้อมูลชีวมิติและข้อมูลส่วนบุคคลจะต้องส่งแยกออกจากกันเท่าที่เป็นไปได้ในการระบุตัวตน ในกรณียืนยันตัวตน ควรส่งข้อมูลชีวมิติของบุคคลและข้อมูลอ้างอิงที่ไม่ใช่ชื่อเพื่อที่จะจำกัดข้อมูลที่จะเป็นอันตรายถ้าข้อมูลทั้งสองถูกดักเก็บไปได้

(4) **การผิดฝาผิดตัว (mismatches)** ควรแก้ไขได้ง่าย เช่น ในกรณีสามีและภรรยาส่งข้อมูลลายนิ้วมือและข้อมูลส่วนตัว แต่ลายนิ้วมือของสามีถูกเก็บไว้ในข้อมูลส่วนตัวของภรรยา และกลับกัน หรือกรณีลายนิ้วมือของคนเดียวกันที่นิ้วชี้เก็บที่นิ้วกลางและสลับกัน

(5) **การชดเชย (redress)** เป็นสิ่งทีสำคัญมากถ้าบุคคลอ้างว่าข้อมูลไม่ถูกต้อง ซึ่งข้อมูลสามารถถูกตรวจสอบและทำให้ถูกต้องได้ถ้ามีความเหมาะสม

เมื่อสร้างระบบการเก็บข้อมูลชีวมิติ การป้องกันสิทธิส่วนบุคคลควรจะสร้างไปพร้อมกันตั้งแต่เริ่มต้น การประเมินผลกระทบสิทธิส่วนบุคคล (PIA) ได้มุ่งเป้าไปในประเด็นที่ต้องสืบสวนที่ควรจะดำเนินการดังต่อไปนี้

- การเก็บรวบรวมสารสนเทศ (information collection)
- การใช้สารสนเทศ (information use)
- การเก็บรักษาสารสนเทศ (information retention)
- การแลกเปลี่ยนสารสนเทศภายในและภายนอก (internal and external information sharing)
- คำเตือน (notice)
- การเข้าถึงข้อมูลส่วนบุคคล การชดเชย การแก้ไขให้ถูกต้อง (individual access, redress, and correction)
- ความปลอดภัย (security)
- เทคโนโลยี (technology)

สำหรับรายละเอียดเกี่ยวกับการใช้งานชีวมิติและสิทธิส่วนบุคคลมีอยู่ในมาตรฐาน ISO/IEC TR 24714-1;2008 [31] และมาตรฐาน ISO/IEC 29100:2011 [32]

## 9. ข้อเสนอแนะการประยุกต์ใช้งานมาตรฐานเพื่อการพิสูจน์และยืนยันตัวตน

ในส่วนนี้จะเป็นข้อเสนอแนะการประยุกต์ใช้งานมาตรฐานที่กล่าวไปแล้วก่อนหน้า โดยจะสาธิตการนำมาตรฐานเกี่ยวกับการใช้เทคโนโลยีชีวมิติไปประยุกต์ใช้งานการบริหารอัตลักษณ์บุคคล เพื่อให้เกิดประสิทธิภาพสูงสุด มีความแม่นยำ และเป็นที่เชื่อถือได้ ซึ่งจะประกอบด้วยกระบวนการดังต่อไปนี้

(1) การลงทะเบียนชีวมิติในระบบรู้จำชีวมิติอัตโนมัติ

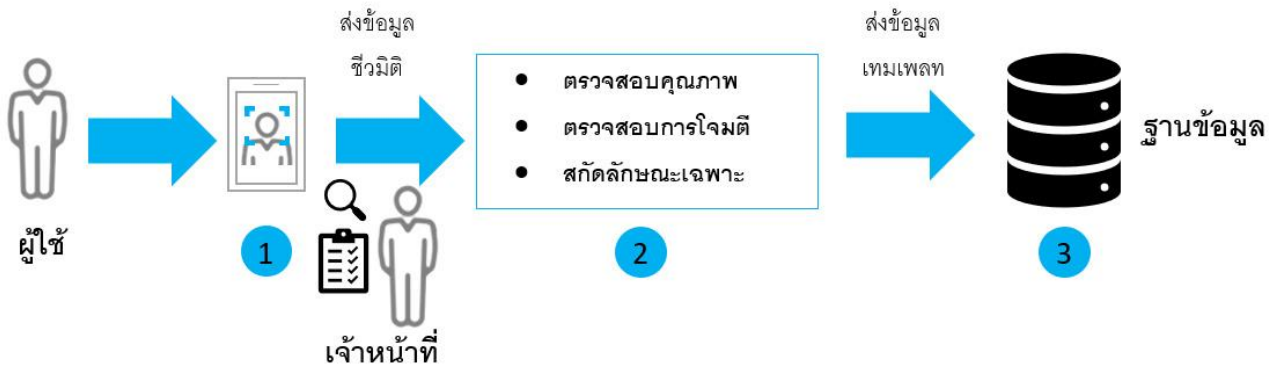
(2) การพิสูจน์ยืนยันตัวตนด้วยชีวมิติกับระบบรู้จำชีวมิติอัตโนมัติ

(3) การพิสูจน์ยืนยันตัวตนด้วยเจ้าหน้าที่และระบบรู้จำชีวมิติอัตโนมัติ

(4) การระบุตัวตนด้วยชีวมิติกับเจ้าหน้าที่และระบบรู้จำชีวมิติอัตโนมัติ

โดยมีรายละเอียดในแต่ละกระบวนการดังต่อไปนี้

### 9.1 การลงทะเบียนชีวมิติในระบบรู้จำชีวมิติอัตโนมัติ




**รูปที่ 6 ผังงานการลงทะเบียนชีวมิติในระบบรู้จำชีวมิติอัตโนมัติ**

การลงทะเบียนด้วยชีวมิติ ดังแสดงในรูปที่ 6 โดยอธิบายขั้นตอนตามตัวเลข ดังต่อไปนี้

(1) ผู้ใช้ที่ต้องการลงทะเบียนในระบบจะแสดงชีวมิติ ที่ระบบเก็บข้อมูลเพื่อเก็บข้อมูลตัวอย่างชีวมิติ หลังจากการผ่านการพิสูจน์ยืนยันตัวตนจากเจ้าหน้าที่ว่าเป็นเจ้าของอัตลักษณ์หรือหลักฐานแสดงตนที่กล่าวอ้างอย่างแท้จริง จึงส่งข้อมูลตัวอย่างชีวมิติเข้าระบบ

(2) จากนั้นระบบจะประมวลผลข้อมูลตัวอย่างชีวมิติ ซึ่งจะเกี่ยวข้องกับ การตรวจสอบคุณภาพ การตรวจจับการโจมตีหลอก การสกัดลักษณะสำคัญชีวมิติเพื่อสร้างเทมเพลตชีวมิติ หากตรวจพบการโจมตีหลอกหรือข้อมูลมีคุณภาพต่ำระบบจะปฏิเสธการลงทะเบียนและให้ผู้ใช้ส่งข้อมูลตัวอย่างชีวมิติเข้ามาใหม่

(3) เทมเพลตชีวมิติและข้อมูลตัวอย่างชีวมิติ จะถูกส่งไปจัดเก็บและลงทะเบียนในฐานข้อมูล ซึ่งข้อมูลตัวอย่างชีวมิติจะเปลี่ยนเป็นข้อมูลอ้างอิงชีวมิติในฐานข้อมูลชีวมิติ

โดยอ้างอิงจากข้อเสนอแนะและมาตรฐานที่กล่าวไว้ก่อนหน้า สามารถกำหนดข้อเสนอแนะได้ดังต่อไปนี้

**(1) การบันทึกข้อมูลตัวอย่างชีวมิติ** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 5.3, 6.1 และ 6.2

**(2) การวัดคุณภาพข้อมูลตัวอย่างชีวมิติ** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 6.3

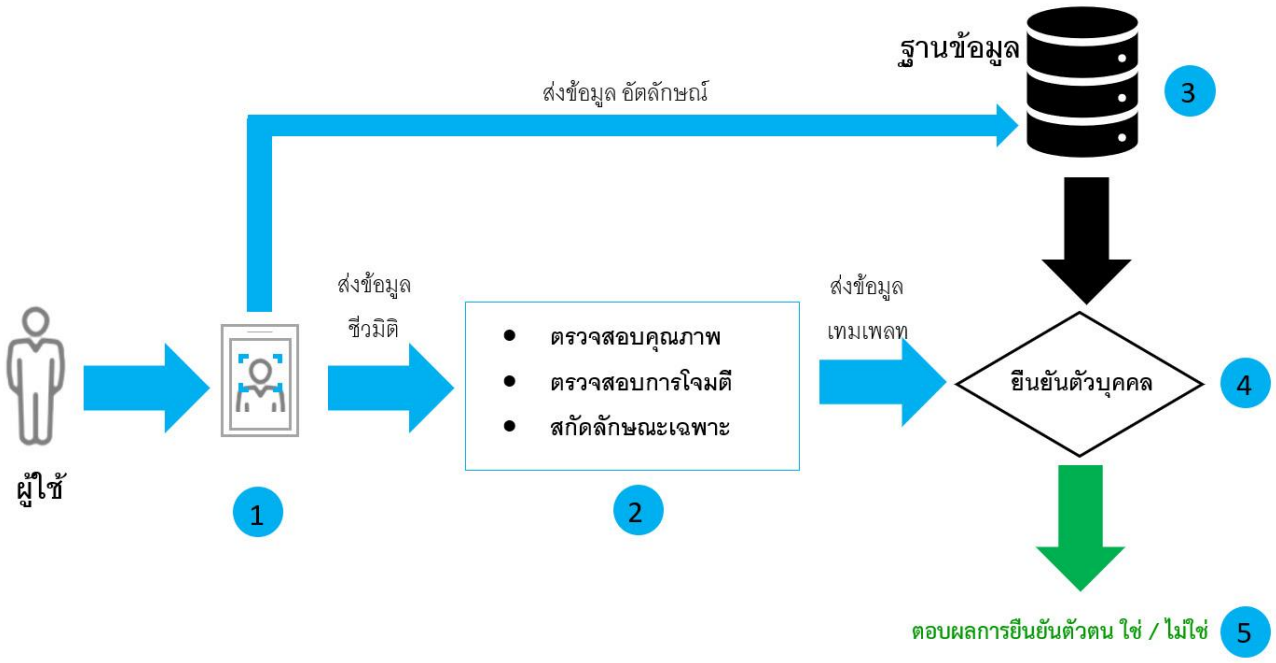
**(3) การป้องกันการโจมตีหลอก** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 7.1

**(4) การระบุตัวตนเพื่อป้องกันระเบียนซ้ำ** ในการลงทะเบียนควรมีการตรวจสอบเพื่อป้องกันการลงทะเบียนซ้ำ ตามข้อเสนอแนะในหัวข้อที่ 6.1 (10)

**(5) ตัวอย่างนโยบายการลงทะเบียน** เช่น ในการลงทะเบียนอาจกำหนดให้เก็บข้อมูลตัวอย่างชีวมิติหลายครั้งเพื่อเลือกข้อมูลตัวอย่างชีวมิติที่ดีที่สุด ซึ่งจะให้ค่าคะแนนคุณภาพสูงที่สุด หรืออาจใช้การรวมข้อมูลตัวอย่างชีวมิติเพื่อให้ข้อมูลชีวมิติมีคุณภาพดีขึ้นได้

**(6) การบันทึกข้อมูลอ้างอิงชีวมิติและการสร้างเทมเพลต** การบันทึกข้อมูลอ้างอิงชีวมิติควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 6.2 และการสร้างเทมเพลตควรมีการป้องกันตามข้อเสนอแนะในหัวข้อที่ 7.2 ซึ่งการเก็บข้อมูลอ้างอิงชีวมิติกับเทมเพลตชีวมิติ ควรเก็บแยกกันคนละหน่วยงานเพื่อป้องกันการผูกขาดจากผู้ให้บริการเทคโนโลยีชีวมิติ

## 9.2 การพิสูจน์ยืนยันตัวตนด้วยชีวมิติกับระบบรู้จำชีวมิติอัตโนมัติ




**รูปที่ 7 ผังงานการพิสูจน์ยืนยันตัวตนด้วยชีวมิติกับระบบรู้จำชีวมิติอัตโนมัติ**

การทำงานลักษณะนี้เป็นการเปรียบเทียบชีวมิติแบบหนึ่งต่อหนึ่ง (one-to-one) โดยใช้ระบบรู้จำชีวมิติอัตโนมัติทำการพิสูจน์ยืนยันตัวตน ไม่มีเจ้าหน้าที่มาเกี่ยวข้อง ดังแสดงในรูปที่ 7 โดยอธิบายขั้นตอนตามตัวเลขดังต่อไปนี้

(1) ผู้ใช้ที่ต้องการพิสูจน์ยืนยันตัวตนจะแสดงชีวมิติของตนที่เซนเซอร์เก็บข้อมูลตัวอย่างชีวมิติเพื่อเก็บข้อมูลพร้อมกับให้รหัสอ้างอิงตัวตน ซึ่งรหัสอ้างอิงนี้อาจอยู่ในรูปแบบ สมาร์ทการ์ด (smart card) อาร์เอฟไอดี (RFID) บาร์โค๊ด (barcode) พินโค๊ด (pin code) หรือ รหัสผ่าน (password) หรือ รูปแบบอื่น ๆ ตามความเหมาะสมในการใช้งาน

(2) จากนั้นระบบจะประมวลผลข้อมูลตัวอย่างชีวมิติ ซึ่งจะเกี่ยวข้องกับ การตรวจสอบคุณภาพ การตรวจจับการโจมตีหลอก การสกัดลักษณะสำคัญชีวมิติเพื่อสร้างเทมเพลตชีวมิติ หากตรวจพบการโจมตีหลอกหรือข้อมูลมีคุณภาพต่ำระบบจะปฏิเสธการลงทะเบียนและให้ผู้ใช้ส่งข้อมูลตัวอย่างชีวมิติเข้ามาใหม่

(3) ระบบจะดึงข้อมูลเทมเพลตชีวมิติจากฐานข้อมูลตามรหัสอ้างอิง เทมเพลตชีวมิติที่ได้นี้ถูกสกัดจากข้อมูลอ้างอิงชีวมิติของผู้ที่ลงทะเบียนไว้

(4) ระบบจะเปรียบเทียบเทมเพลตอ้างอิงชีวมิติจากฐานข้อมูลและเทมเพลตชีวมิติจากผู้ใช้

(5) ถ้าคะแนนความเหมือนเกินกว่าค่าเทรชโฮลด์ที่ตั้งไว้ ระบบจะตอบผลลัพธ์การเปรียบเทียบเป็น “ใช่” ถ้าคะแนนความเหมือนต่ำกว่า ระบบจะตอบ “ไม่ใช่”

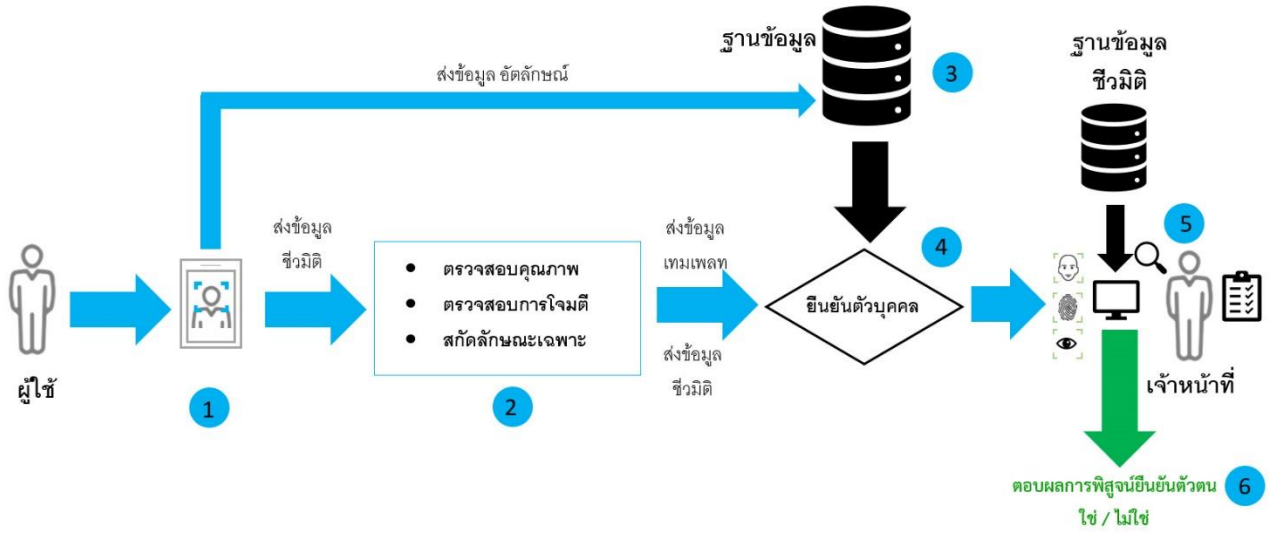
โดยอ้างอิงจากข้อเสนอแนะและมาตรฐานที่กล่าวไว้ก่อนหน้า สามารถกำหนดข้อเสนอแนะได้ดังต่อไปนี้

**(1) การวัดคุณภาพข้อมูลตัวอย่างชีวมิติ** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 6.3

**(2) การป้องกันการโจมตีหลอก** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 7.1

**(3) ตัวอย่างนโยบายการพิสูจน์ยืนยันตัวตน** ในการพิสูจน์ยืนยันตัวตนอาจกำหนดให้ตัดสินผลลัพธ์การเปรียบเทียบเทมเพลตชีวมิติจากข้อมูลอ้างอิงชีวมิติและจากผู้ใช้บริการ โดยการพิจารณาผลลัพธ์คะแนนความเหมือนปัจจัยเดียว หรือ อาจให้พิจารณาค่าคุณภาพร่วมด้วย และระบบที่ใช้ชีวมิติหลายประเภท เช่น ระบบรู้จำใบหน้าและลายม่านตา อาจกำหนดให้ตัดสินผลลัพธ์จากการพิจารณาค่าคะแนนความเหมือนจากชีวมิติหลายประเภทร่วมกัน

## 9.3 การพิสูจน์ยืนยันตัวตนด้วยเจ้าหน้าที่และระบบรู้จำชีวมิติอัตโนมัติ




**รูปที่ 8 ผังงานการพิสูจน์ยืนยันตัวตนด้วยเจ้าหน้าที่และระบบรู้จำชีวมิติอัตโนมัติ**

การทำงานลักษณะนี้เป็นการเปรียบเทียบชีวมิติแบบหนึ่งต่อหนึ่ง (one-to-one) โดยใช้ระบบรู้จำชีวมิติอัตโนมัติร่วมกับเจ้าหน้าที่ทำการพิสูจน์ยืนยันตัวตนดังแสดงในรูปที่ 8 ซึ่งจะใช้ในกรณีที่มีปัญหาไม่สามารถพิสูจน์ยืนยันตัวตนผ่านระบบได้โดยผู้ใช้ยืนยันว่าเป็นบุคคลที่กล่าวอ้างจริง เจ้าหน้าที่จะทำงานร่วมกับระบบรู้จำชีวมิติเพื่อแก้ไขปัญหา โดยอธิบายขั้นตอนตามตัวเลข ดังต่อไปนี้

(1) ผู้ใช้ที่ต้องการพิสูจน์ยืนยันตัวตนจะแสดงชีวมิติของตนที่เซนเซอร์เก็บข้อมูลตัวอย่างชีวมิติเพื่อเก็บข้อมูลพร้อมกับให้รหัสอ้างอิงตัวตน ซึ่งรหัสอ้างอิงนี้อาจอยู่ในรูปแบบ สมาร์ทการ์ด (smart card) อาร์เอฟไอดี (RFID) บาร์โค๊ด (barcode) พินโค๊ด (pin code) หรือ รหัสผ่าน (password) หรือ รูปแบบอื่น ๆ ตามความเหมาะสมในการใช้งาน

(2) จากนั้นระบบจะประมวลผลข้อมูลตัวอย่างชีวมิติ ซึ่งจะเกี่ยวข้องกับ การตรวจสอบคุณภาพ การตรวจจับการโจมตีหลอก การสกัดลักษณะสำคัญชีวมิติเพื่อสร้างเทมเพลตชีวมิติ หากตรวจพบการโจมตีหลอกหรือข้อมูลมีคุณภาพต่ำระบบจะปฏิเสธการลงทะเบียนและให้ผู้ใช้ส่งข้อมูลตัวอย่างชีวมิติเข้ามาใหม่

(3) ระบบจะดึงข้อมูลเทมเพลตชีวมิติจากฐานข้อมูลตามรหัสอ้างอิง เทมเพลตชีวมิติที่ได้นี้ถูกสกัดจากข้อมูลอ้างอิงชีวมิติของผู้ที่ลงทะเบียนไว้

(4) ระบบจะเปรียบเทียบเทมเพลตอ้างอิงชีวมิติจากฐานข้อมูลและเทมเพลตชีวมิติจากผู้ใช้

(5) เจ้าหน้าที่จะทำการตรวจสอบข้อมูลอ้างอิงชีวมิติในฐานข้อมูลชีวมิติเปรียบเทียบกับข้อมูลตัวอย่างชีวมิติที่ได้จากผู้ใช้ ผลจากการพิสูจน์ยืนยันตัวตนโดยใช้ระบบรู้จำชีวมิติอัตโนมัติ ร่วมกับหลักฐานแสดงตนหรือข้อมูลอัตลักษณ์อื่น ๆ ที่สามารถพิสูจน์และยืนยันตัวตนของผู้ใช้ได้อย่างมั่นใจ ว่าเป็นบุคคลที่เป็นเจ้าของอัตลักษณ์จริง ๆ

(6) เจ้าหน้าที่จะตอบผลลัพธ์การเปรียบเทียบเป็น ใช่หรือไม่ใช่

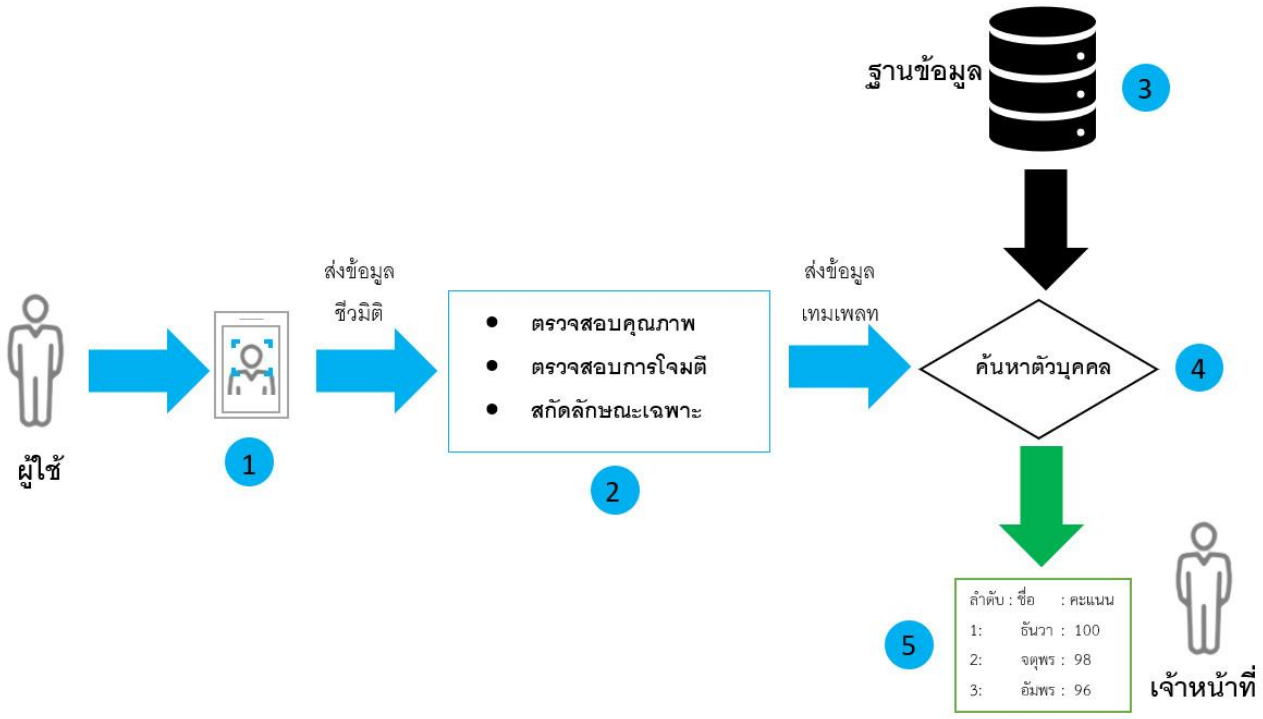
โดยอ้างอิงจากข้อเสนอแนะและมาตรฐานที่กล่าวไว้ก่อนหน้า สามารถกำหนดข้อเสนอแนะได้ดังต่อไปนี้

**(1) การวัดคุณภาพข้อมูลชีวมิติ** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 6.3

**(2) การป้องกันการโจมตีหลอก** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 7.1

**(3) ตัวอย่างนโยบายการพิสูจน์ยืนยันตัวตนด้วยเจ้าหน้าที่** ในการพิสูจน์ยืนยันตัวตนที่ต้องใช้เจ้าหน้าที่จะใช้เฉพาะกรณีที่มีการลงทะเบียนครั้งแรก หรือเวลาที่มีปัญหาระบบรู้จำชีวมิติอัตโนมัติทำงานผิดพลาดปฏิเสธตัวตนของผู้ใช้ตัวจริง ในกรณีเหล่านี้ จำเป็นต้องใช้เจ้าหน้าที่พิจารณาเปรียบเทียบข้อมูลอ้างอิงชีวมิติที่เก็บไว้ในฐานข้อมูลชีวมิติเพื่อนำมาเปรียบเทียบกับข้อมูลตัวอย่างชีวมิติของผู้ใช้ และอาจมีความจำเป็นที่ต้องใช้หลักฐานข้อมูลอัตลักษณ์ส่วนบุคคลอื่น ๆ ประกอบการตัดสินใจเพื่อพิสูจน์ยืนยันตัวตนของผู้ใช้ได้อย่างมั่นใจ และสามารถรับรองโดยเจ้าหน้าที่ รวมทั้งรวมรวมปัญหาที่เกิดขึ้นเพื่อแก้ไขระบบให้สามารถลดความผิดพลาดและใช้งานได้อย่างมีประสิทธิภาพสูงสุดต่อไป

## 9.4 การระบุตัวตนด้วยชีวมิติกับเจ้าหน้าที่และระบบรู้จำชีวมิติอัตโนมัติ




**รูปที่ 9 ผังงานการระบุตัวตนด้วยชีวมิติกับเจ้าหน้าที่และระบบรู้จำชีวมิติอัตโนมัติ**

การทำงานลักษณะนี้เป็นการเปรียบเทียบชีวมิติแบบหนึ่งต่อกลุ่ม (one-to-many) ดังแสดงในรูปที่ 9 โดยอธิบายขั้นตอนตามตัวเลข ดังต่อไปนี้

(1) ผู้ใช้จะแสดงชีวมิติของตนที่เซนเซอร์เก็บข้อมูลตัวอย่างชีวมิติเพื่อเก็บข้อมูล

(2) จากนั้นระบบจะประมวลผลข้อมูลตัวอย่างชีวมิติ ซึ่งจะเกี่ยวข้องกับ การตรวจสอบคุณภาพ การตรวจจับการโจมตีหลอก การสกัดลักษณะสำคัญชีวมิติเพื่อสร้างเทมเพลตชีวมิติ หากตรวจพบการโจมตีหลอกหรือข้อมูลมีคุณภาพต่ำระบบจะปฏิเสธการลงทะเบียนและให้ผู้ใช้ส่งข้อมูลตัวอย่างชีวมิติเข้ามาใหม่

(3) ระบบจะดึงเทมเพลตอ้างอิงชีวมิติทั้งหมดจากฐานข้อมูล

(4) ระบบจะเปรียบเทียบเทมเพลตชีวมิติจากผู้ใช้กับเทมเพลตอ้างอิงชีวมิติทั้งหมดในฐานข้อมูลและให้ผลลัพธ์เป็นคะแนนความเหมือนของทุกคู่การเปรียบเทียบ จากนั้นระบบตัดสินใจจะกำหนดผลลัพธ์จากคะแนนความเหมือนเป็น รายการบุคคล (candidate list) ที่เรียงลำดับรายการตามคะแนนความเหมือนซึ่งเรียงจากมากไปน้อย โดยอันดับที่ 1 คือเทมเพลตอ้างอิงชีวมิติที่เปรียบเทียบได้คะแนนความเหมือนสูงที่สุด

(5) ระบบจะตอบผลลัพธ์ผู้ที่ได้คะแนนความเหมือนสูงสุด หรือตอบเป็นรายการบุคคลตามจำนวนรายการที่กำหนด เช่น รายการบุคคล 10 ลำดับแรกที่มีคะแนนความเหมือนสูงสุด หรือไม่พบบุคคลที่ค้นหา

โดยอ้างอิงจากข้อเสนอแนะและมาตรฐานที่กล่าวไว้ก่อนหน้า สามารถกำหนดข้อเสนอแนะได้ดังต่อไปนี้

**(1) การวัดคุณภาพข้อมูลชีวมิติ** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 6.3

**(2) การป้องกันการโจมตีหลอก** ควรเป็นไปตามข้อเสนอแนะในหัวข้อที่ 7.1

**(3) ตัวอย่างนโยบายการระบุตัวตน** ในการระบุตัวตนอาจกำหนดให้ตัดสินผลลัพธ์รายการบุคคลจากการพิจารณาผลลัพธ์คะแนนความเหมือนปัจจัยเดียว หรือ อาจให้พิจารณาค่าคุณภาพข้อมูลชีวมิติร่วมด้วย หรือ อาจให้พิจารณาคะแนนความเหมือนจากชีวมิติหลายประเภทร่วมกัน ในกรณีที่เป็นระบบที่ใช้ชีวมิติหลายตำแหน่ง (multi-instance) เช่น การใช้ตาซ้ายและตาขวาร่วมกัน มือซ้ายและมือขวาร่วมกัน นิ้ว 10 นิ้วร่วมกัน ระบบอาจนำผลลัพธ์รายการบุคคลที่ได้จากแต่ละตำแหน่งมารวมเป็นผลลัพธ์รายการบุคคลสุดท้ายและระบุบุคคลที่ค้นหา (ถ้ามี)

## บรรณานุกรม


[1] ขมธอ. 18-2564 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (เวอร์ชัน 2.0)

[2] ขมธอ. 19-2564 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (เวอร์ชัน 2.0)

[3] ขมธอ. 20-2564 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (เวอร์ชัน 2.0)

[4] International Organization for Standardization, “ISO/IEC 2382-37, Information technology — Vocabulary — Part 37: Biometrics”, February 2017.

[5] International Organization for Standardization, “ISO/IEC 24760-1:2019 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts”, May 2019.

[6] International Organization for Standardization, “ISO/IEC TR 29144:2014 Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes”, July 2014.

[7] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, สมุดปกขาว “การพิสูจน์และยืนยันตัวตนด้วยระบบไบโอเมตริก,” โครงการพัฒนามาตรฐานการใช้งานเทคโนโลยีชีวมิติ (Biometric Standard) สำหรับการพิสูจน์และยืนยันตัวตน, พ.ศ. 2564

[8] International Organization for Standardization, “ISO/IEC TR 30110:2015 Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children”, November 2015.

[9] L. Best-Rowden and A. K. Jain, “Longitudinal study of automatic face recognition,” IEEE transactions on pattern analysis and machine intelligence, 40(1), pp. 148-162, 2017.

[10] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[11] ANNUAL REPORT, Unique Identification Authority of India, 2019-2020 https://uidai.gov.in/images/AADHAR_AR_2019_20_ENG_approved.pdf

[12] International Organization for Standardization, “ISO/IEC 39794-1:2019 Information technology — Extensible biometric data interchange formats — Part 1: Framework”, December 2019.

[13] International Organization for Standardization, “ISO/IEC 39794-4:2019 Information technology — Extensible biometric data interchange formats — Part 4: Finger image data”, December 2019.

[14] International Organization for Standardization, “ISO/IEC 39794-5:2019 Information technology — Extensible biometric data interchange formats — Part 5: Face image data”, December 2019.

[15] International Organization for Standardization, “ISO/IEC 39794-6:2021 Information technology — Extensible biometric data interchange formats — Part 6: Iris image data”, March 2021.

[16] International Organization for Standardization, “ISO/IEC 39794-9:2021 Information technology — Extensible biometric data interchange formats — Part 9: Vascular image data”, June 2021.

[17] International Organization for Standardization, “ISO/IEC 19794-1:2011 Information technology — Biometric data interchange formats — Part 1: Framework”, July 2011.

[18] International Organization for Standardization, “ISO/IEC 19794-7:2021 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data”, October 2021.

[19] International Organization for Standardization, “ISO/IEC 19794-13:2018 Information technology -- Biometric data interchange formats -- Part 13: Voice data”, March 2018.

[20] International Organization for Standardization, “ISO/IEC 19794-14:202X Information Technology — Biometric Data Interchange Formats — Part 14 - DNA Data”, To be appeared.

[21] International Organization for Standardization, “ISO/IEC 29794-1:2016 Information technology — Biometric sample quality — Part 1: Framework”, January 2016.

[22] International Organization for Standardization, “ISO/IEC 29794-4:2017 Information technology — Biometric sample quality — Part 4: Finger image data”, September 2017.

[23] International Organization for Standardization, “ISO/IEC 29794-5:2010 Information technology — Biometric sample quality — Part 5: Face image data”, April 2010.

[24] International Organization for Standardization, “ISO/IEC 29794-6:2015 Biometric sample quality - Part 6: Iris image data”, July 2015.

[25] พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540

[26] International Organization for Standardization, “ISO/IEC 19785-1:2020 Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification”, September 2020.

[27] A. Rungchokanun, W. Chaidee, C. Deerada, and V. Areekul, “Effect of Pre-Enhancement on False-Rejection Cases of Fingerprint Verification System,” the 1 7 th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2020), pp. 291-295, 2020.

[28] International Organization for Standardization, “ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework”, March 2016.

[29] International Organization for Standardization, “ISO/IEC 19794-2:2011Information technology — Biometric data interchange formats — Part 2: Finger minutiae data”, December 2011.

[30] International Organization for Standardization, “ISO/IEC 30136:2018 Information technology — Performance testing of biometric template protection schemes”, March 2018.

[31] International Organization for Standardization, “ISO/IEC TR 24714-1:2008 Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance”, December 2008.

[32] International Organization for Standardization, “ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework”, December 2011.