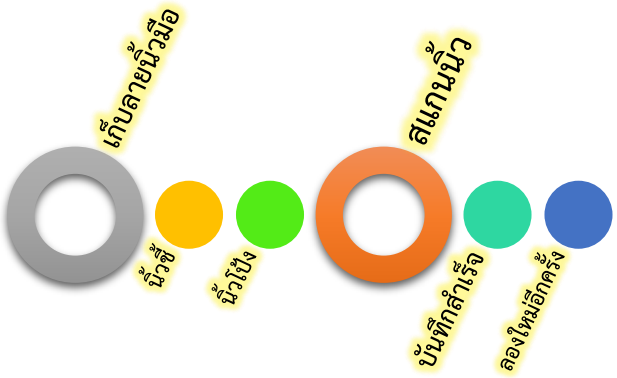
คู่มือการปฏิบัติงาน

ระบบสแกนลายนิ้วมือ

เพื่อลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์



นางสาวประไพศรี เหล่าทองมีสกุล

ตำแหน่ง เจ้าหน้าที่วิเคราะห์ระบบงานคอมพิวเตอร์

ศูนย์เทคโนโลยีดิจิทัล

มหาวิทยาลัยวลัยลักษณ์

คู่มือการปฏิบัติงาน
ระบบสแกนลายนิ้วมือ
เพื่อลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์

นางสาวประไพศรี เหล่าทองมีสกุล

ตำแหน่ง เจ้าหน้าที่วิเคราะห์ระบบงานคอมพิวเตอร์

ศูนย์เทคโนโลยีดิจิทัล

มหาวิทยาลัยวลัยลักษณ์

คำนำ

คู่มือการปฏิบัติงานระบบสแกนลายนิ้วมือฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางในการปฏิบัติงานด้านการใช้งานระบบสแกนลายนิ้วมือของศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์ โดยเนื้อหาของคู่มือการปฏิบัติงาน ประกอบด้วย ความสำคัญของคู่มือการปฏิบัติงาน วัตถุประสงค์ หน้าที่รับผิดชอบ หลักเกณฑ์การปฏิบัติงาน วิธีการปฏิบัติงาน เป้าหมายในการปฏิบัติงาน เทคนิคในการวางแผน/แผน กลยุทธ์ในการปฏิบัติงาน เทคนิคการประเมินผลการปฏิบัติงาน เทคนิคการทำให้ผู้รับบริการพึงพอใจ จรรยาบรรณ/คุณธรรม/จริยธรรมในการปฏิบัติงาน ปัญหาอุปสรรคในการปฏิบัติงาน แนวทางแก้ไข และข้อเสนอแนะ ซึ่งครอบคลุมทุกมิติของการปฏิบัติงาน โดยคู่มือฉบับนี้ได้ใช้งานมาตั้งแต่ปี พ.ศ. 2560 และได้แก้ไขปรับปรุงครั้งล่าสุดเมื่อเดือนตุลาคม 2564 ช่วยให้การปฏิบัติงานเป็นไปแบบมีระบบและเป็นมาตรฐานเดียวกัน เพื่อเพิ่มประสิทธิภาพในการทำงานและเป็นแนวปฏิบัติสำหรับผู้รับผิดชอบที่มารับงานใหม่นี้ใช้เป็นคู่มือในการปฏิบัติงานรวมทั้งอาจจะเป็นแนวทางในการนำไปปรับปรุงพัฒนาระบบงานให้มีประสิทธิภาพยิ่งขึ้นในลำดับถัดไป ผู้เขียนขอขอบคุณคณะวิทยากร เจ้าหน้าที่ที่เกี่ยวข้องในการจัดอบรมหลักสูตรพัฒนาการเขียนคู่มือการปฏิบัติงานของส่วนทรัพยากรมนุษย์และองค์กร มหาวิทยาลัยวลัยลักษณ์ ที่ให้การสนับสนุนจัดเวทีแลกเปลี่ยนเรียนรู้และให้คำแนะนำ จนกระทั่งคู่มือฉบับนี้เสร็จสมบูรณ์

นางสาวประไพศรี เหล่าทองมีสกุล
ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์
26 พฤษภาคม 2565

สารบัญ

หน้า

คำนำ ..... ก
สารบัญ ..... ข
สารบัญตาราง ..... ง
สารบัญภาพ ..... จ
บทที่ 1 บทนำ 1

1.1 ความสำคัญ/ความจำเป็น (ภูมิหลัง) 1
1.2 วัตถุประสงค์ของการศึกษา 3
1.3 ประโยชน์ของการศึกษา 3
1.4 ขอบเขตของการศึกษา 3
1.5 คำนิยาม/คำจำกัดความ 4

บทที่ 2 หน้าที่ความรับผิดชอบและโครงสร้างการบริหารจัดการ 5

2.1 หน้าที่ความรับผิดชอบ 5
2.2 โครงสร้างการบริหารจัดการ 5

ภาพที่ 2.1 โครงสร้างองค์กร (Organization Chart) 8
ภาพที่ 2.2 โครงสร้างการบริหาร (Administration Chart) 9
ภาพที่ 2.3 โครงสร้างการปฏิบัติการ (Active Chart) 10

บทที่ 3 หลักเกณฑ์ วิธีการปฏิบัติงานและเงื่อนไข 11

3.1 หลักเกณฑ์การปฏิบัติงาน 11
3.2 วิธีการปฏิบัติงาน 18
3.3 เงื่อนไข/ข้อสังเกต/ข้อควรระวัง/สิ่งที่ควรคำนึงในการปฏิบัติงาน 35
3.4 แนวคิด/งานวิจัยที่เกี่ยวข้อง 35

บทที่ 4 เป้าหมายและเทคนิคในการปฏิบัติงานแบบมุ่งผลสัมฤทธิ์ 38

4.1 เป้าหมายในการปฏิบัติงาน (ตัวชี้วัดในการปฏิบัติงาน) 38
4.2 เทคนิคในการวางแผน/แผนกลยุทธ์ในการปฏิบัติงาน 39
4.3 เทคนิคในการปฏิบัติงานแต่ละขั้นตอนการปฏิบัติงาน 39
4.4 เทคนิคการติดตามและประเมินผลการปฏิบัติงาน 74
4.5 เทคนิคการทำให้ผู้รับบริการพึงพอใจ 74
4.6 จรรยาบรรณ/คุณธรรม/จริยธรรมในการปฏิบัติงาน 76

บทที่ 5 ปัญหา อุปสรรค แนวทางแก้ไข การพัฒนาและข้อเสนอแนะ 78

5.1 ปัญหาอุปสรรคในการปฏิบัติงานและแนวทางแก้ไข 78
5.2 ข้อเสนอแนะ 82

บรรณานุกรม 83

ภาคผนวก 84
ภาคผนวก 1 ประกาศมหาวิทยาลัยวลัยลักษณ์เรื่องการลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๑ 85
ภาคผนวก 2 ประกาศมหาวิทยาลัยวลัยลักษณ์เรื่องกำหนดเกณฑ์การมาสายของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕ 88
ภาคผนวก 3 ระเบียบมหาวิทยาลัยวลัยลักษณ์ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลามหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๓ 92
ภาคผนวก 4 ประกาศที่ธปท.ฝทง.ว.760/2563 เรื่องนำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ 99
ภาคผนวก 5 มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล 119
ภาคผนวก 6 ข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยประมวลจริยธรรมและธรรมาภิบาลนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕ 177

ประวัติผู้เขียน 186

สารบัญตาราง

ตารางที่ 3.1 แสดงตัวอย่างเวลาปฏิบัติงาน 11

ตารางที่ 3.2 แสดงตัวอย่างเวลาปฏิบัติงานการลาครึ่งวัน.....12

ตารางที่ 3.3 แสดงตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800.....21

ตารางที่ 3.4 แสดงตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone.....30

ตารางที่ 4.1 แผนปฏิบัติการงานระบบสแกนลายนิ้วมือ (Finger Scan).....39

ตารางที่ 4.2 สัญลักษณ์ ชื่อเรียก และความหมายของ Flow chart..... 40

ตารางที่ 5.1 ปัญหา/อุปสรรค แนวทางแก้ไข 80

สารบัญภาพ

ภาพที่ 1.1 ภาพแสดงพนักงานเข้าแถวเพื่อการสแกนลายนิ้วมือ 2
ภาพที่ 2.1 โครงสร้างองค์กร (Organization Chart) 8
ภาพที่ 2.2 โครงสร้างการบริหาร (Administration Chart) 9
ภาพที่ 2.3 โครงสร้างการปฏิบัติการ (Active Chart) 10
ภาพที่ 3.1 เส้นโค้งราบ 13
ภาพที่ 3.2 เส้นโค้งกระโจม 13
ภาพที่ 3.3 มัดหวายปัดขวา 14
ภาพที่ 3.4 มัดหวายปัดซ้าย 14
ภาพที่ 3.5 ก้นหอยธรรมดา 14
ภาพที่ 3.6 ก้นหอยกระเป๋ากลาง 15
ภาพที่ 3.7 ก้นหอยกระเป๋าข้าง 16
ภาพที่ 3.8 แบบซับซ้อน 16
ภาพที่ 3.9 แสดงรูปแบบของลายนิ้วมือ 17
ภาพที่ 3.10 อุปกรณ์เก็บลายนิ้วมือ 18
ภาพที่ 3.11 การลงทะเบียนเก็บลายนิ้วมือ 19
ภาพที่ 3.12 MATCHER รุ่น M-800 20
ภาพที่ 3.13 เครื่องสแกนลายนิ้วมือ รุ่น Standalone 29
ภาพที่ 4.1 ขั้นตอนการปฏิบัติงาน : เมื่อมีพนักงานใหม่เข้ามาทำงาน 41
ภาพที่ 4.2 หน้าจอโปรแกรมบริหารจัดการ Stand Alone Product Management 3.0 42
ภาพที่ 4.3 หน้าจอเกี่ยวกับ Device Management 43
ภาพที่ 4.4 หน้าจอเกี่ยวกับระบบบริหารจัดการอุปกรณ์เพื่อการบันทึกเวลาพนักงาน 43
ภาพที่ 4.5 หน้าจอเกี่ยวกับโปรแกรมบริหารจัดการ Stand Alone Product 44
ภาพที่ 4.6 หน้าจอเกี่ยวกับโปรแกรมบริหารจัดการ Stand Alone Product [บันทึกลายนิ้วมือ] 45
ภาพที่ 4.7 หน้าจอเกี่ยวกับค้นหาพนักงาน 46
ภาพที่ 4.8 หน้าจอเกี่ยวกับผลการค้นหาพนักงาน 46
ภาพที่ 4.9 หน้าจอเกี่ยวกับรายละเอียดของพนักงาน “อรรถพล” 47

สารบัญภาพ(ต่อ)

ภาพที่ 4.10 หน้าจอเกี่ยวกับรายละเอียดกำหนดการใช้งานเครื่องลูกข่ายของ “อรรถพล” 48
ภาพที่ 4.11 หน้าจอเกี่ยวกับผลการบันทึกสำเร็จที่กำหนดการใช้งานเครื่องลูกข่ายของ “อรรถพล” 49
ภาพที่ 4.12 หน้าจอเกี่ยวกับการส่งข้อมูลผู้ใช้รายบุคคล 50
ภาพที่ 4.13 หน้าจอเกี่ยวกับการค้นหาข้อมูลผู้ใช้ 51
ภาพที่ 4.14 หน้าจอเกี่ยวกับการค้นหาข้อมูลผู้ใช้ของ “อรรถพล” 51
ภาพที่ 4.15 หน้าจอเกี่ยวกับการค้นหาพบข้อมูลผู้ใช้ของ “อรรถพล” 52
ภาพที่ 4.16 หน้าจอเกี่ยวกับการส่งข้อมูลผู้ใช้ของ “อรรถพล” 53
ภาพที่ 4.17 หน้าจอเกี่ยวกับการส่งข้อมูลผู้ใช้ของ “อรรถพล” ไปยังรายการที่เลือกไว้ 54
ภาพที่ 4.18 หน้าจอเกี่ยวกับการกดปุ่มตกลงเพื่อดำเนินการส่งข้อมูล 55
ภาพที่ 4.19 หน้าจอเกี่ยวกับระบบกำลังดำเนินการส่งข้อมูล 56
ภาพที่ 4.20 หน้าจอเกี่ยวกับการอ่านข้อมูลเครื่อง 57
ภาพที่ 4.21 หน้าจอเกี่ยวกับรายละเอียดข้อมูลเครื่อง 58
ภาพที่ 4.22 หน้าจอเกี่ยวกับการอ่านข้อมูลเครื่อง 59
ภาพที่ 4.23 หน้าจอเกี่ยวกับผลการอ่านข้อมูลเครื่องสำเร็จ 60
ภาพที่ 4.24 หน้าจอเกี่ยวกับผลการอ่านข้อมูลเครื่องสำเร็จและให้ค้นหา 61
ภาพที่ 4.25 หน้าจอเกี่ยวกับการค้นหา 61
ภาพที่ 4.26 หน้าจอเกี่ยวกับแสดงผลของการค้นหา 62
ภาพที่ 4.27 หน้าจอเกี่ยวกับแสดงเมนูรายงาน 63
ภาพที่ 4.28 หน้าจอเกี่ยวกับแสดงเมนูรายงานการใช้งานตามผู้ใช้ 63
ภาพที่ 4.29 หน้าจอเกี่ยวกับการให้กรอกข้อมูลในเมนูรายงานการใช้งานตามผู้ใช้ 64
ภาพที่ 4.30 หน้าจอเกี่ยวกับแสดงรายงานการใช้งานตามผู้ใช้ 65
ภาพที่ 4.31 หน้าจอเกี่ยวกับแสดงเมนูการพิมพ์รายงานการใช้งานตามผู้ใช้ 66
ภาพที่ 4.32 หน้าจอเกี่ยวกับแสดงเมนูการใส่ค่าจำนวนการสั่งพิมพ์รายงานการใช้งานตามผู้ใช้ 66
ภาพที่ 4.33 หน้าจอเกี่ยวกับแสดงการดึงข้อมูลการลงเวลา 67
ภาพที่ 4.34 หน้าจอเกี่ยวกับแสดงการดึงข้อมูลการลงเวลาที่สำเร็จ 68

สารบัญภาพ(ต่อ)

ภาพที่ 4.35 หน้าจอเกี่ยวกับเว็บระบบสารสนเทศบริหารงานบุคคล 69
ภาพที่ 4.36 หน้าจอเกี่ยวกับเว็บระบบสารสนเทศบริหารงานบุคคลที่ Login เพื่อดูรายงาน 70
ภาพที่ 4.37 หน้าจอเกี่ยวกับการดูรายงานแบบเลือกเดือนที่ต้องการ 71
ภาพที่ 4.38 หน้าจอเกี่ยวกับการดูรายงานแบบเลือกเดือนที่ต้องการ เช่น 2560 กรกฎาคม 72
ภาพที่ 4.39 หน้าจอเกี่ยวกับรายงานแบบเลือกเดือนที่ต้องการ เช่น 2560 กรกฎาคม 73
ภาพที่ 4.40 หน้าจอเกี่ยวกับรายงานการใช้งานตามผู้ใช้ 74
ภาพที่ 4.41 รายงานแสดงรายเดือน 75
ภาพที่ 4.42 รายงานแสดงข้อมูลการสแกนลายนิ้วมือ 76

บทที่ 1
บทนำ

1.1 ความสำคัญ/ความจำเป็น (ภูมิหลัง)

มหาวิทยาลัยวลัยลักษณ์เป็นมหาวิทยาลัยในกำกับของรัฐ ที่จัดการเรียนการสอนครอบคลุมทั้งด้านสังคมศาสตร์ วิทยาศาสตร์และเทคโนโลยี และวิทยาศาสตร์สุขภาพ โดยพัฒนาสภาพแวดล้อมให้เป็นเมืองมหาวิทยาลัยที่มีระบบสาธารณูปโภคและสาธารณูปการแบบครบวงจร รวมทั้งสิ่งอำนวยความสะดวกอื่นๆ มีการจัดภูมิทัศน์ให้เป็นแหล่งเรียนรู้ภายใต้สิ่งแวดล้อมที่ดี มีภารกิจหลัก 4 ด้าน (ศูนย์เทคโนโลยีดิจิทัล, 2564)

1) ผลิตและพัฒนากำลังคนระดับสูงให้มีมาตรฐานที่สอดคล้องกับความต้องการในการพัฒนาเศรษฐกิจและสังคมในภาคใต้และของประเทศ

2) ดำเนินการศึกษา ค้นคว้า วิจัยและพัฒนาองค์ความรู้ใหม่ให้สามารถนำไปใช้ในการผลิตให้มีคุณภาพและประสิทธิภาพ เพื่อความสามารถในการพึ่งตนเองและการแข่งขันในระดับนานาชาติ

3) ให้บริการทางวิชาการแก่หน่วยงานต่างๆ ทั้งภาครัฐและเอกชนในด้านการให้คำปรึกษา แนะนำการวิจัยและพัฒนา การทดสอบ การสำรวจ รวมทั้งการฝึกอบรม อันก่อให้เกิดการถ่ายทอดเทคโนโลยีที่จำเป็นและเหมาะสม เพื่อการพัฒนาเศรษฐกิจและสังคมของภูมิภาคและประเทศชาติ

4) อนุรักษ์และฟื้นฟูศิลปะและวัฒนธรรมอันเป็นจารีตประเพณี รวมทั้งศิลปะบริสุทธิ์และศิลปะประยุกต์ เพื่อให้มหาวิทยาลัยเป็นศูนย์รวมของชุมชนและเป็นแบบอย่างที่ดีของสังคม

โดยกำหนดวิสัยทัศน์ว่าเป็นองค์การธรรมรัฐ เป็นแหล่งเรียนรู้ เป็นหลักในถิ่น เป็นเลิศสู่สากล (มหาวิทยาลัยวลัยลักษณ์ ส่วนแผนงานและยุทธศาสตร์, 2560, น. 50-51) มหาวิทยาลัยมียุทธศาสตร์การพัฒนาระยะยาว 20 ปี (พ.ศ. 2561-2580) และหนึ่งในยุทธศาสตร์การพัฒนาระยะยาว 20 ปี คือ ยุทธศาสตร์ที่ 2 การพัฒนาองค์กรและบริหารทุนมนุษย์ มุ่งสู่องค์กรสมรรถนะสูง ซึ่งต้องมีการบริหารจัดการงานที่รวดเร็ว ทันสมัยและมุ่งเน้นผลงาน จำเป็นอย่างยิ่งที่องค์กรต้องเตรียมส่งเสริมและพัฒนาการใช้ระบบสารสนเทศให้เป็นเครื่องมือในการบริหารจัดการที่มีประสิทธิภาพสูงสุด เพื่อนำไปสู่การเป็น Paperless Office

จากวิสัยทัศน์เชื่อมโยงมาถึงยุทธศาสตร์การพัฒนาองค์กรและบริหารทุนมนุษย์ มุ่งสู่องค์กรสมรรถนะสูง เพื่อให้บรรลุผลตามที่มหาวิทยาลัยวางแผนไว้ ศูนย์เทคโนโลยีดิจิทัลมีความพร้อมและได้สนับสนุนการพัฒนาระบบสารสนเทศที่มีความเหมาะสมในการใช้งานของมหาวิทยาลัยรวมถึงการมีระบบสารสนเทศของงานระบบสแกนลายนิ้วมือ (Finger Scan)

ปัญหาที่ผ่านมาพนักงานหรือลูกจ้างสายปฏิบัติการวิชาชีพและบริหารทั่วไป ได้ใช้วิธีการเสียบบัตรสมาร์ตการ์ด เพื่อลงเวลาเข้าปฏิบัติงานและลงเวลาออกปฏิบัติงาน มีลักษณะที่สามารถฝากให้เพื่อนพนักงานนำมาเสียบบัตรแทนกันได้ ทำให้ส่วนทรัพยากรมนุษย์และองค์กรของมหาวิทยาลัย ไม่สามารถตรวจสอบได้ว่า พนักงานได้เข้าทำงานจริงในแต่ละวันที่มาทำงาน ด้วยพนักงานของหน่วยงานนั้นๆ ก็ไม่ได้อยู่ในอาคารเดียวกันกับส่วนทรัพยากรมนุษย์และองค์กร จึงได้หาแนวทางแก้ไขปัญหาดังกล่าวเป็นรูปแบบใหม่เพื่อแก้ปัญหาการฝากบัตรมาเสียบแทน นั่นคือ การนำเทคโนโลยีที่เรียกว่าระบบการสแกนลายนิ้วมือเพื่อลงเวลาการปฏิบัติงาน

การสแกนลายนิ้วมือในมหาวิทยาลัยวลัยลักษณ์สำหรับพนักงานและลูกจ้างสายปฏิบัติการวิชาชีพและบริหารทั่วไป รวมทั้งสิ้น 1,779 คน (มหาวิทยาลัยวลัยลักษณ์ ส่วนทรัพยากรมนุษย์และองค์กร, 2565) เพื่อเป็นการแสดงตนของพนักงานในการลงเวลาเข้าปฏิบัติงานและลงเวลาออกปฏิบัติงาน โดยประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง การลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. 2561 กำหนดให้พนักงานกลุ่มตำแหน่งปฏิบัติการวิชาชีพและบริหารทั่วไปและกลุ่มตำแหน่งบริหารจัดการ ประกอบด้วย หัวหน้างาน หัวหน้าฝ่าย หัวหน้าสำนักงาน ต้องลงเวลาปฏิบัติงานด้วยการสแกนลายนิ้วมือ (ภาพที่ 1.1) กรณีพนักงานกลุ่มตำแหน่งปฏิบัติการวิชาชีพและบริหารทั่วไปและกลุ่มตำแหน่งบริหารจัดการไม่ลงเวลาปฏิบัติงาน ถือว่าเป็นการฝ่าฝืน ไม่ปฏิบัติตามนโยบาย ข้อบังคับ ระเบียบ และธรรมเนียมปฏิบัติที่มหาวิทยาลัยกำหนดอาจมีความผิดทางวินัย

ภาพที่ 1.1 ภาพแสดงพนักงานเข้าแถวเพื่อการสแกนลายนิ้วมือ

ศูนย์เทคโนโลยีดิจิทัล เป็นหน่วยงานที่มีหน้าที่ดูแลการบริหารจัดการอุปกรณ์เครื่องสแกนลายนิ้วมือให้กับส่วนทรัพยากรมนุษย์และองค์กรของมหาวิทยาลัยวลัยลักษณ์ เพื่อบรรลุผลอย่างถูกต้องของการออกรายงานการมาปฏิบัติงานของพนักงานและลูกจ้างสายปฏิบัติการวิชาชีพและ

บริหารทั่วไป ในระบบสารสนเทศบริหารงานบุคคล โดยที่ระบบสแกนลายนิ้วมือเริ่มติดตั้งให้ใช้งานในปี พ.ศ. 2551 จนถึงปัจจุบันรวมระยะเวลากว่า 14 ปี มีอุปกรณ์เครื่องสแกนลายนิ้วมือ ที่สามารถสแกนลายนิ้วมือเพื่อลงเวลาการปฏิบัติงานได้ทั้งหมด 35 จุด ทั้งในเขตการศึกษาและนอกเขตการศึกษา พบว่า ยังมีการแจ้งกรณีพนักงานไม่สามารถสแกนลายนิ้วมือเพื่อการเข้างาน การออกงาน ทำให้เกิดปัญหาข้อมูลรายงานการมาปฏิบัติงานไม่ถูกต้อง

จากความสำคัญและความจำเป็นดังกล่าวข้างต้น จึงนำมาเขียนเป็นคู่มือการปฏิบัติงาน เรื่อง ระบบสแกนลายนิ้วมือเพื่อลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ เพื่อใช้เป็นคู่มือปฏิบัติงาน เพื่อให้เพื่อนผู้ปฏิบัติงานทำงานทดแทนกันได้และปฏิบัติงานในมาตรฐานเดียวกัน

1.2 วัตถุประสงค์ของการศึกษา

(1) เพื่อใช้เป็นคู่มือปฏิบัติงานสำหรับผู้ดูแลระบบ (Admin) ด้านระบบสแกนลายนิ้วมือ และให้ผู้ปฏิบัติงานสามารถทำงานแทนกันได้และเป็นมาตรฐานเดียวกัน
(2) เพื่อให้ผู้ที่เกี่ยวข้องมีความรู้ความเข้าใจเกี่ยวกับระบบสแกนลายนิ้วมือ

1.3 ประโยชน์ของการศึกษา

(1) ได้คู่มือปฏิบัติงานเพื่อใช้ในการปฏิบัติงานสำหรับผู้ดูแลระบบ (Admin) ด้านระบบสแกนลายนิ้วมือ ผู้ปฏิบัติงานทำงานทดแทนกันได้และเป็นมาตรฐานเดียวกัน
(2) ผู้ที่เกี่ยวข้องมีความรู้ความเข้าใจเกี่ยวกับระบบสแกนลายนิ้วมือ

1.4 ขอบเขตของการศึกษา

คู่มือนี้ใช้สำหรับผู้ปฏิบัติงานในฐานะ Admin ด้านการใช้งานระบบสแกนลายนิ้วมือ กำหนดเป็นขอบเขต ได้แก่

(1) การนำเข้าข้อมูลพนักงานใหม่
(2) การตรวจสอบพร้อมปรับแก้ข้อมูลให้ถูกต้อง
(3) การกำหนดสิทธิ์ให้กับพนักงานใหม่
(4) การส่งข้อมูลสิทธิ์ให้กับพนักงานใหม่
(5) การทดสอบการใช้งาน
(6) การนำเข้าข้อมูลการลงเวลาปฏิบัติงาน
(7) การรายงานการลงเวลาปฏิบัติงาน

1.5 คำนิยาม/คำจำกัดความ

มหาวิทยาลัย	หมายถึง	มหาวิทยาลัยวลัยลักษณ์
ศูนย์เทคโนโลยีดิจิทัล	หมายถึง	ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์
ส่วนทรัพยากรมนุษย์และองค์กร	หมายถึง	ส่วนทรัพยากรมนุษย์และองค์กร มหาวิทยาลัยวลัยลักษณ์
ระบบสารสนเทศบริหารงานบุคคล	หมายถึง	ระบบสารสนเทศบริหารงานบุคคล มหาวิทยาลัยวลัยลักษณ์
พนักงาน	หมายถึง	พนักงานสายปฏิบัติการวิชาชีพและบริหารทั่วไป มหาวิทยาลัยวลัยลักษณ์
ลูกจ้าง	หมายถึง	ลูกจ้างสายปฏิบัติการวิชาชีพและบริหารทั่วไป มหาวิทยาลัยวลัยลักษณ์
Finger Scan	หมายถึง	เครื่องสแกนลายนิ้วมือ
Enrollment	หมายถึง	การลงทะเบียนเก็บบันทึกลายนิ้วมือแม่แบบ
เทคโนโลยีชีวมิติ (Biometric technology)	หมายถึง	**เทคโนโลยีที่ใช้ในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรมของบุคคล เช่น การ พูด การเขียน เพื่อระบุพิสูจน์หรือยืนยันตัวตนบุคคล ความถูกต้องของตัวบุคคล (ธนาคารแห่งประเทศไทย, 2563)**

บทที่ 2
หน้าที่ความรับผิดชอบและโครงสร้างการบริหารจัดการ

2.1 หน้าที่ความรับผิดชอบ

ปฏิบัติงานในตำแหน่งเจ้าหน้าที่วิเคราะห์ระบบงานคอมพิวเตอร์ ระดับปฏิบัติการ สังกัดฝ่ายวิจัยและพัฒนาระบบสารสนเทศ ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์ ด้วยศูนย์เทคโนโลยีดิจิทัลเป็นหน่วยงานที่ให้บริการและประสานภารกิจมีหน้าที่สนับสนุน Hardware และ Software ให้กับหน่วยงานภายในของมหาวิทยาลัยตั้งแต่ปี พ.ศ. 2541 ซึ่งเป็นปีแรกที่เริ่มเปิดการเรียนการสอนแล้วนั้น อีกหนึ่งภาระงานของการสนับสนุนช่วยให้ส่วนทรัพยากรมนุษย์และองค์กร สามารถดำเนินงานเพื่อการบริหารจัดการในด้านงานพัฒนาระบบบริหารบุคคล งานบริหารทั่วไปและธุรการ มีความสะดวกคล่องตัว รวดเร็ว สามารถออกรายงานการลงเวลาปฏิบัติงานของพนักงานและลูกจ้าง ในระบบสารสนเทศบริหารงานบุคคลได้อย่างถูกต้องแม่นยำ จากที่กล่าวมาข้างต้น งานระบบ Finger Scan จึงต้องรับผิดชอบและให้การสนับสนุน 2 ด้าน ได้แก่

2.1.1 ดูแลอุปกรณ์ด้าน Hardware ของตัวเครื่อง

งานดูแลอุปกรณ์ด้าน Hardware ของตัวเครื่อง คือ การบำรุงรักษาให้เครื่องสแกนลายนิ้วมือรวม 35 เครื่อง ต้องทำงานได้ 24 ชั่วโมงของทุกวัน การซ่อมเครื่องสแกนลายนิ้วมือที่ได้รับแจ้งว่าไม่สามารถใช้งานได้ การดำเนินการติดตั้งเครื่องสแกนลายนิ้วมือตัวใหม่ในอาคารที่เพิ่งจะเปิดใช้งาน การดำเนินการย้ายเครื่องสแกนลายนิ้วมือในอาคารเดิมไปอาคารแห่งใหม่ตามที่มีคำขอมาที่ศูนย์เทคโนโลยีดิจิทัล

2.1.2 การใช้งานระบบโปรแกรมบริหารจัดการ

เป็นการใช้งานโปรแกรมบริหารจัดการสำหรับระบบ Finger Scan โดยผู้เป็น Admin ต้องรู้รายละเอียดของเมนูหลักในระบบ เริ่มตั้งแต่การเข้าสู่ระบบ เมนูข้อมูล เมนูเครื่องลูกข่าย เมนูเครื่องมือ และเมนูรายงาน

2.2 โครงสร้างการบริหารจัดการ

ศูนย์เทคโนโลยีดิจิทัลเป็นหน่วยงานหนึ่งของมหาวิทยาลัยวลัยลักษณ์ที่จัดตั้งขึ้นโดยวัตถุประสงค์เพื่อเป็นหน่วยงานรวมบริการประสานและให้บริการงานคอมพิวเตอร์และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อรองรับการบริหารจัดการงานวิชาการและงานบริการของหน่วยงานต่างๆ ในมหาวิทยาลัย ประสานและดำเนินการพัฒนาระบบงานสารสนเทศและซอฟต์แวร์ประยุกต์ จัดบริการงานคอมพิวเตอร์และให้การฝึกอบรมทางคอมพิวเตอร์แก่บุคลากรภายในและหน่วยงานภายนอก ประสานและจัดบริการงานคอมพิวเตอร์เพื่อการเรียนการสอน ตรวจสอบและบำรุงรักษาเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ รวมถึงปฏิบัติงานอื่นๆ ที่มหาวิทยาลัยมอบหมาย

2.2.1 โครงสร้างองค์กร (Organization Chart) ตามประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง การแบ่งส่วนงานของสำนักงานอธิการบดี สำนักวิชา สถาบัน ศูนย์ หรือหน่วยงานที่เรียกชื่ออย่างอื่น พ.ศ. 2565 ได้แบ่งส่วนงานเป็น 4 ฝ่าย ประกอบด้วย (1) ฝ่ายบริหารทั่วไปและธุรการ (2) ฝ่ายวิจัยและพัฒนาระบบสารสนเทศ (3) ฝ่ายบริการระบบเครือข่ายและสื่อสาร และ (4) ฝ่ายบริการและฝึกอบรมเทคโนโลยีดิจิทัล โครงสร้างองค์กรของศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์ (ภาพที่ 2.1)

2.2.2 โครงสร้างการบริหาร (Administration Chart) ตามคำสั่งมหาวิทยาลัยวลัยลักษณ์ที่ 652/2565 เรื่อง โครงสร้างการสั่งการและการกำกับดูแล ให้ผู้ช่วยศาสตราจารย์ ดร.ณิชนันทน์ กิตติพัฒนบวร รักษาการแทนผู้ช่วยอธิการบดี กำกับดูแลศูนย์เทคโนโลยีดิจิทัล โดยผู้อำนวยการและรองผู้อำนวยการเป็นผู้บริหารขององค์กรระดับสูง มีหัวหน้าฝ่าย 4 ฝ่าย เป็นผู้บริหารขององค์กรระดับกลาง ดูแลรับผิดชอบงานย่อยภายในฝ่าย โครงสร้างบริหารงานศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์ (ภาพที่ 2.2)

2.2.3 โครงสร้างการปฏิบัติการ (Active Chart) มีโครงสร้างปฏิบัติการ ประกอบด้วย 4 ฝ่าย คือ (1) ฝ่ายบริหารทั่วไปและธุรการ (2) ฝ่ายวิจัยและพัฒนาระบบสารสนเทศ (3) ฝ่ายบริการระบบเครือข่ายและสื่อสาร และ (4) ฝ่ายบริการและฝึกอบรมเทคโนโลยีดิจิทัล (ภาพที่ 2.3) โดยแต่ละฝ่ายจะมีกรอบภาระงานดังนี้

1) ฝ่ายบริหารทั่วไปและธุรการ แบ่งเป็น 2 งานย่อย ได้แก่

1.1) งานธุรการและบริหารทั่วไป

มีหน้าที่ความรับผิดชอบเกี่ยวกับการรับ-ส่งหนังสือ ร่างโต้ตอบหนังสือ จัดพิมพ์หนังสือหรือเอกสาร จัดเก็บรักษาและรวบรวมเอกสาร ระเบียบต่าง ๆ ของมหาวิทยาลัย และของศูนย์/สถาบัน/สำนัก เสนอทำลายหนังสือหรือเอกสารของศูนย์/สถาบัน/สำนัก ประสานการดำเนินการจัดทำงบประมาณของหน่วยงาน แผนงานเกี่ยวกับการจัดซื้อจัดจ้าง และเบิกจ่ายพัสดุจัดทำบัญชีควบคุมการเบิกจ่ายเงินสดย่อยของหน่วยงาน ควบคุมพัสดุ ประสานงานด้านประชาสัมพันธ์และการประชุมต่าง ๆ

1.2) งานบริหารสำนักงานและลูกค้าสัมพันธ์

มีหน้าที่ความรับผิดชอบเกี่ยวกับการดำเนินการประสานงานกับหน่วยงานภายในและภายนอกและฝ่ายต่าง ๆ ภายในศูนย์ เพื่อให้บริการที่เกี่ยวข้องกับการเรียนการสอน การวิจัย ตลอดจนติดตามและประเมินผลงานในการให้บริการการเรียนการสอน การวิจัยเพื่อนำมาปรับปรุงแก้ไขการให้บริการดังกล่าวให้เหมาะสมยิ่งขึ้น

2) ฝ่ายวิจัยและพัฒนาระบบสารสนเทศ แบ่งเป็น 3 งานย่อย ได้แก่

2.1) งานพัฒนาระบบสนับสนุนการเรียนการสอน การวิจัย

ทำหน้าที่พัฒนาระบบสารสนเทศหรือระบบงานหรือ Application ที่เกี่ยวข้องกับการเรียนการสอน การวิจัย การบริการวิชาการ และการทำนุบำรุงศิลปะและวัฒนธรรม เช่น ระบบ e-Learning ระบบ e-Testing ระบบสารสนเทศผลการปฏิบัติงานพนักงานสาย

ปฏิบัติการระบบสารสนเทศผลการปฏิบัติงานพนักงาสายวิชาการ ระบบทะเบียนงานวิจัย ระบบทะเบียนงานบริการวิชาการ ระบบทะเบียนงานทำนุบำรุงศิลปะและวัฒนธรรม ระบบแสดงความคิดเห็นต่อการสอนของอาจารย์ ระบบบันทึก มคอ. เป็นต้น

2.2) งานพัฒนาระบบสนับสนุนการบริหารงาน

ทำหน้าที่พัฒนาระบบสารสนเทศ หรือระบบงาน หรือ Application ที่เกี่ยวข้องกับการบริหารงานภายในมหาวิทยาลัย เช่น เว็บไซต์มหาวิทยาลัย เว็บไซต์หน่วยงาน/สำนักวิชา งานบริหารทรัพยากรบุคคล งานการเงิน งานพัสดุ งานระบบบริหารจัดการสำนักงานดิจิทัล ระบบ e-Meeting งานระบบ Finger Scan เป็นต้น

2.3) งานพัฒนาระบบงบประมาณ พัสดุ การเงินและบัญชี แบบสามมิติ

ทำหน้าที่เกี่ยวกับการดูแลและพัฒนาระบบงานงบประมาณ พัสดุ การเงินและบัญชี แบบสามมิติ

3) ฝ่ายบริการระบบเครือข่ายและสื่อสาร แบ่งเป็น 2 งานย่อย ได้แก่

3.1) งานระบบเครือข่าย

ให้บริการระบบโครงสร้างพื้นฐาน เครือข่ายสายให้กับพนักงานและนักศึกษาเพื่อรองรับงานด้านการเรียนการสอน การปฏิบัติงานด้านสารสนเทศ งานวิจัย และงานอื่น ๆ ของมหาวิทยาลัย

3.2) งานระบบสื่อสาร

ให้บริการระบบโครงสร้างพื้นฐานเครือข่ายไร้สาย ให้กับนักศึกษาเพื่อรองรับ ด้านการเรียนการสอน การสืบค้นข้อมูล งานวิจัย และด้านอื่นๆ ที่จำเป็นต้องใช้ระบบเครือข่ายไร้สายในการเข้าถึงข้อมูล

4) ฝ่ายบริการและฝึกอบรมเทคโนโลยีดิจิทัล แบ่งเป็น 2 งานย่อย ได้แก่

4.1) งานบริการคอมพิวเตอร์เพื่องานสำนักงาน

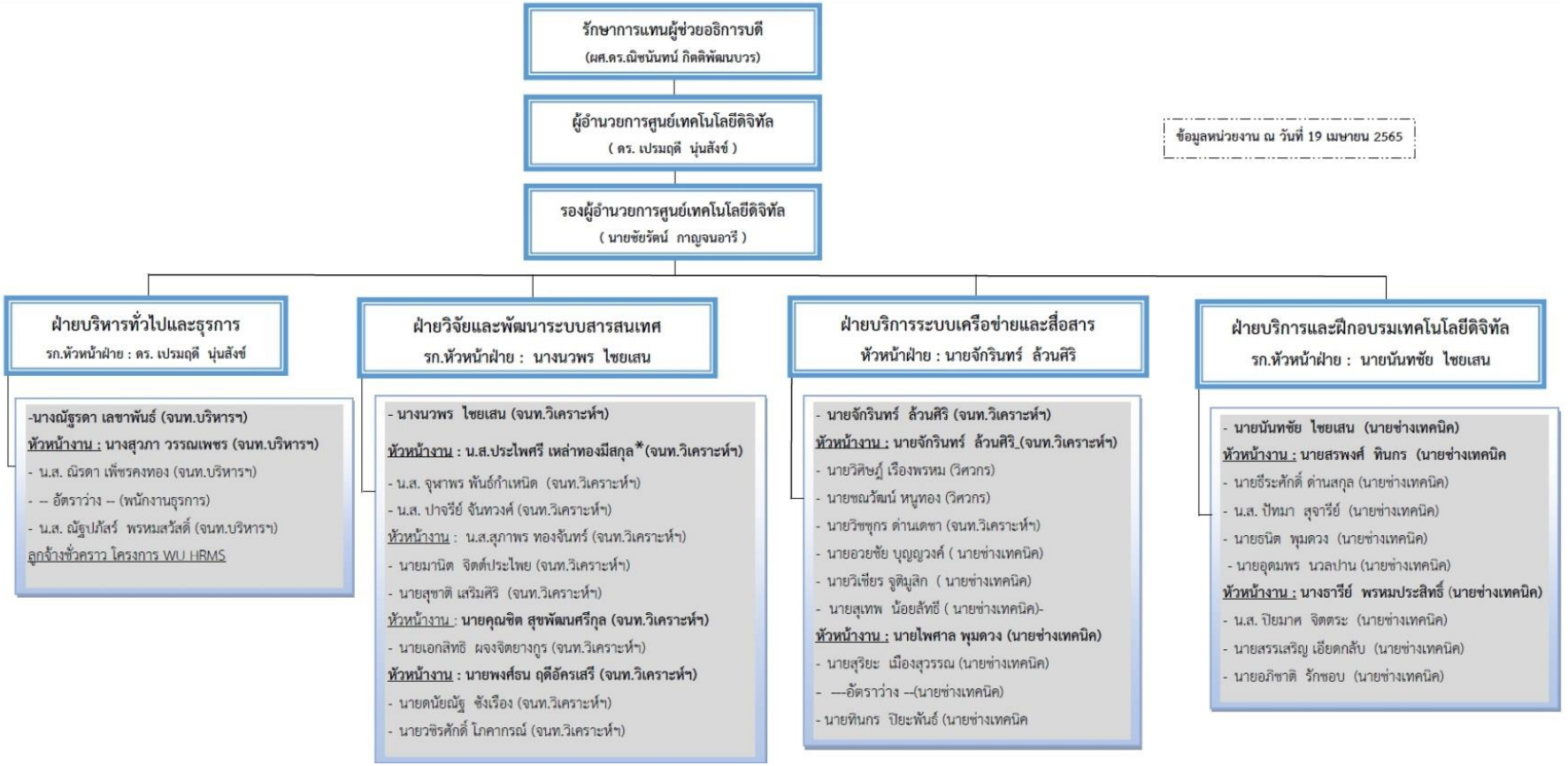
ทำหน้าที่ในการให้บริการซ่อมบำรุงและติดตั้งอุปกรณ์คอมพิวเตอร์เพื่อการใช้งานคอมพิวเตอร์ในสำนักงานของหน่วยงานภายในมหาวิทยาลัย

4.2) งานบริการคอมพิวเตอร์เพื่อการเรียนการสอน

ทำหน้าที่ในการให้บริการซ่อมบำรุงและดูแลอุปกรณ์คอมพิวเตอร์เพื่อการใช้งานเกี่ยวกับการเรียนการสอน

ภาพที่ 2.1 โครงสร้างองค์กร (Organization Chart)

ภาพที่ 2.2 โครงสร้างการบริหาร (Administration Chart)



ภาพที่ 2.3 โครงสร้างการปฏิบัติการ (Active Chart)

*** หมายเหตุ นางสาวประไพศรี เหล่าทองมีสกุล ผู้เขียนคู่มือปฏิบัติงาน**

บทที่ 3
หลักเกณฑ์ วิธีการปฏิบัติงานและเงื่อนไข

3.1 หลักเกณฑ์การปฏิบัติงาน

ในปี พ.ศ. 2551 คณะผู้บริหารของมหาวิทยาลัยวลัยลักษณ์ได้เลือกให้มีวิธีการลงเวลาปฏิบัติงานของพนักงานและลูกจ้าง ด้วยการสแกนลายนิ้วมือแทนการใช้บัตรสมาร์ตการ์ด โดยมีหลักเกณฑ์การปฏิบัติงานในลักษณะสำคัญตามลำดับ เริ่มจาก (1) การนำเข้าข้อมูลพนักงานใหม่ (2) การตรวจสอบพร้อมปรับแก้ข้อมูลให้ถูกต้อง (3) การกำหนดสิทธิ์ให้กับพนักงานใหม่ (4) การส่งข้อมูลสิทธิ์ให้กับพนักงานใหม่ (5) การทดสอบการใช้งาน (6) การนำเข้าข้อมูลการลงเวลาปฏิบัติงาน (7) การรายงานการลงเวลาปฏิบัติงาน โดยขั้นตอนที่ (1) ถึง (7) จะทำงานได้แบบสมบูรณ์ต้องสัมพันธ์กับรูปแบบที่กำหนดไว้ดังนี้

1) การลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ ต้องบันทึกเวลาเข้าและออกการปฏิบัติงานด้วยการสแกนลายนิ้วมือ วันละ 2 ครั้ง สามารถลงเวลาได้ทุกอาคารที่ติดตั้งเครื่องสแกนลายนิ้วมือเพื่อลงเวลาปฏิบัติงาน

2) เกณฑ์การมาสายของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พนักงานและลูกจ้างต้องลงเวลาปฏิบัติงานตามเวลาที่กำหนด ดังตัวอย่างเวลาปฏิบัติงาน

ตารางที่ 3.1 แสดงตัวอย่างเวลาปฏิบัติงาน

เวลาทำงาน	ลงเวลาเข้า	ลงเวลาออก
08.30 - 16.30 น.	ภายในเวลา 08.30 น. หากลงเวลา หลัง 08.30 น. ถือว่ามาสาย	หลังเวลา 16.30 น. หากลงเวลา ก่อน 16.30 น. ถือว่าออกก่อน
08.00 - 16.00 น.	ภายในเวลา 08.00 น. หากลงเวลา หลัง 08.00 น. ถือว่ามาสาย	หลังเวลา 16.00 น. หากลงเวลา ก่อน 16.00 น. ถือว่าออกก่อน
14.00 - 22.00 น.	ภายในเวลา 14.00 น. หากลงเวลา หลัง 14.00 น. ถือว่ามาสาย	หลังเวลา 22.00 น. หากลงเวลา ก่อน 22.00 น. ถือว่าออกก่อน

การลาครึ่งวัน ต้องลงเวลาปฏิบัติงานตามเวลาที่กำหนด ยกตัวอย่างเวลาปฏิบัติงาน ดังนี้

ตารางที่ 3.2 แสดงตัวอย่างเวลาปฏิบัติงานการลาครึ่งวัน

เวลาทำงาน	การลา	ลงเวลาเข้า	ลงเวลาออก
08.30-16.30 น.	ลาครึ่งวันเช้า เข้าทำงานครึ่งวันบ่าย	ภายในเวลา 13.00 น. หากลงเวลาหลัง 13.00 น. ถือว่ามาสาย	หลังเวลา 16.30 น. หากลงเวลาก่อน 16.30 น. ถือว่าออกก่อน
08.30-16.30 น.	ลาครึ่งวันบ่าย เข้าทำงานครึ่งวันเช้า	ภายในเวลา 08.30 น. หากลงเวลาหลัง 08.30 น. ถือว่ามาสาย	หลังเวลา 12.00 น. หากลงเวลาก่อน 12.00น. ถือว่าออกก่อน
08.00-16.00 น.	ลาครึ่งวันเช้า เข้าทำงานครึ่งวันบ่าย	ภายในเวลา 12.30 น. หากลงเวลาหลัง 12.30 น. ถือว่ามาสาย	หลังเวลา 16.00 น. หากลงเวลาก่อน 16.00 น. ถือว่าออกก่อน
08.00-16.00 น.	ลาครึ่งวันบ่าย เข้าทำงานครึ่งวันเช้า	ภายในเวลา 08.00 น. หากลงเวลาหลัง 08.00 น. ถือว่ามาสาย	หลังเวลา 11.30 น. หากลงเวลาก่อน 11.30 น. ถือว่าออกก่อน
14.00-22.00 น.	ลาครึ่งวันเช้า เข้าทำงานครึ่งวันบ่าย	ภายในเวลา 18.30 น. หากลงเวลาหลัง 18.30 น. ถือว่ามาสาย	หลังเวลา 22.00 น. หากลงเวลาก่อน 22.00 น. ถือว่าออกก่อน
14.00-22.00 น.	ลาครึ่งวันบ่าย เข้าทำงานครึ่งวันเช้า	ภายในเวลา 14.00 น. หากลงเวลาหลัง 14.00 น. ถือว่ามาสาย	หลังเวลา 17.30 น. หากลงเวลาก่อน 17.30 น. ถือว่าออกก่อน

กรณีพนักงานและลูกจ้างไม่ลงเวลาเข้าหรือออกจากการทำงานให้ถือเป็นการมาสาย รวมถึงการออกก่อนก็ให้นับเป็นการมาสายเช่นเดียวกัน

3) เกณฑ์การจัดเวลาทำงานและการทำงานล่วงเวลา ให้จัดการทำงานเป็นกะ สำหรับงานที่มีลักษณะปฏิบัติงานต่อเนื่องต้องปฏิบัติงานไม่น้อยกว่า 16 ชั่วโมง เช่น การปฏิบัติงาน 16 ชั่วโมง ให้จัดเป็น 2 กะ หรือ 24 ชั่วโมง ให้จัดเป็น 3 กะ เป็นต้น และให้จัดตารางทำงานแบบเหลื่อมเวลา โดยให้มีเวลาทำงาน 8 ชั่วโมงต่อวัน (รวมเวลาหยุดพักหนึ่งชั่วโมง) เช่น 07.30-15.30 น. หรือ 08.30-16.30 น. หรือ 12.00-20.00 น. เป็นต้น

4) รูปแบบของลายนิ้วมือ ที่สามารถเก็บลักษณะได้ แบ่งเป็น 4 แบบ (ชัยรัตน์ องค์วิศิษฐ์. 2548, น. 10) ได้แก่

4.1) แบบเส้นโค้ง (Arch) แบ่งออกเป็น 2 ชนิดย่อย ดังนี้

4.1.1) แบบโค้งราบ (Plain Arch) ตัวเส้นลายนิ้วมือจะวิ่งหรือไหลออกไปข้างหนึ่ง โดยจะไม่เกิดมุมแหลม หรือ พุ่งขึ้นตรงกลาง

ภาพที่ 3.1 เส้นโค้งราบ

4.1.2) แบบโค้งกระโจม (Tented Arch) ตัวเส้นลายนิ้วมือตรงกลางจะมีลักษณะเป็นเส้นพุ่งขึ้นจากแนวนอนเป็นมุมแหลมหรือมุมฉาก

ภาพที่ 3.2 เส้นโค้งกระโจม

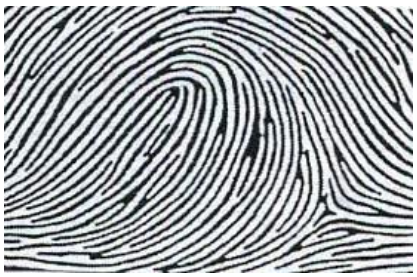
4.2) แบบมัดหวาย (Loop)

ลายนิ้วมือแบบมัดหวาย เป็นรูปแบบลายนิ้วมือที่พบมากที่สุดในทุกเชื้อชาติ คือ ประมาณ 65% ของลายนิ้วมือทั้งหมด แบ่งออกเป็น 2 ชนิดย่อย ดังนี้

4.2.1) แบบมัดหวายปัดขวา (Right Loop) ลายนิ้วมือจะมีจุดสันดอนเพียงจุดเดียว และมีเส้นวกหลักที่สมบูรณ์อย่างน้อย 1 เส้น โดยมีทิศทางไปทางขวา

ภาพที่ 3.3 มัดหวายปัดขวา

4.2.2) แบบมัดหวายปัดซ้าย (Left Loop) ลายนิ้วมือจะมีจุดสันดอนเพียงจุดเดียว และมีเส้นวกหลักที่สมบูรณ์อย่างน้อย 1 เส้น โดยมีทิศทางไปทางซ้าย



ภาพที่ 3.4 มัดหวายปัดซ้าย

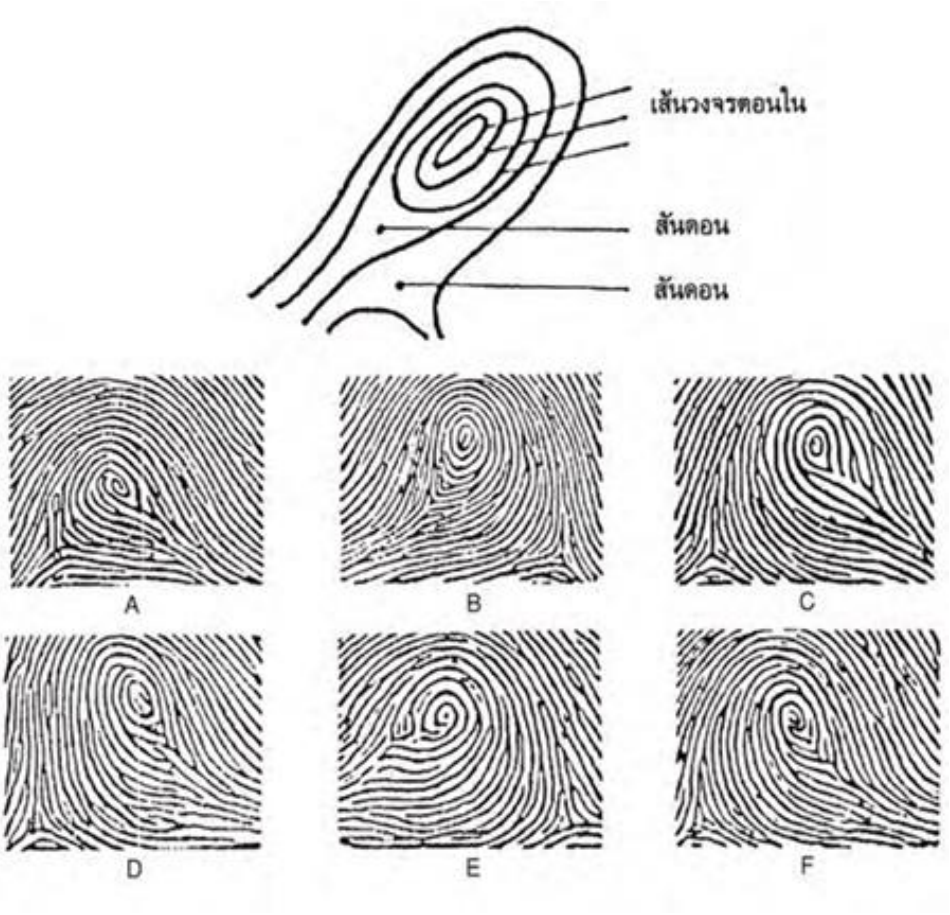
4.3) แบบก้นหอย (Whorl)

ลายนิ้วมือแบบก้นหอย สามารถพบได้ประมาณ 30 % จากลายนิ้วมือทั้งหมด ซึ่งสามารถสังเกตได้โดยจะมีเส้นลายนิ้วมืออย่างน้อย 1 เส้น ที่เป็นเส้นเวียนรอบเป็นวงคล้ายกับก้นหอย แบ่งได้เป็น 3 ชนิดย่อย คือ

4.3.1) แบบก้นหอยธรรมดา (Plain Whorl) เป็นรูปแบบเส้นลายนิ้วมือที่มีการไหลของเส้นเวียนรอบเป็นวงจร อาจวนคล้ายนาฬิกา หรือวงกลม

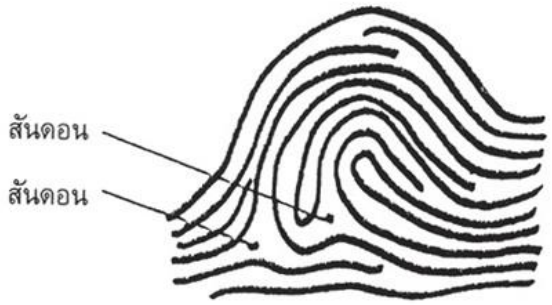
ภาพที่ 3.5 ก้นหอยธรรมดา

4.3.2) แบบก้นหอยกระเป๋ากลาง (Central Pocket) เป็นรูปแบบเส้นลายนิ้วมือที่มีการไหลของเส้นคล้ายแบบก้นหอยธรรมดา ต่างกันตรงที่หากลากเส้นสมมติเชื่อมระหว่างสันดอนทั้งสองจุดจะพบว่าไม่สัมผัสเส้นวงจรที่อยู่ด้านในของวง หรือมีส่วนปัดของวงอยู่ในแนวตรงกลางนิ้วมือ



ภาพที่ 3.6 ก้นหอยกระเป๋ากลาง

4.3.3) แบบก้นหอยกระเป๋าข้าง (lateral Pocket) เป็นรูปแบบเส้นลายนิ้วมือที่มีการไหลคล้ายแบบก้นหอยธรรมดา แต่มีส่วนปัดของวงหันไปทางด้านซ้ายหรือด้านขวาของนิ้วมือ



ภาพที่ 3.7 ก้นหอยกระเป๋าข้าง

4.4) แบบซับซ้อน (Accidental Whorl)

ลายนิ้วมือแบบซับซ้อน เป็นลายนิ้วมือที่มีรูปแบบลักษณะพิเศษ ที่ไม่ใช่ลายนิ้วมือทั้ง 3 แบบที่กล่าวมา หรืออาจจะเป็นลายนิ้วมือ 2 แบบ มารวมกัน หรืออาจเป็น 3 แบบมารวมกัน ซึ่งลักษณะโดยทั่วไปจะมีรูปแบบที่ไม่แน่นอน

ภาพที่ 3.8 แบบซับซ้อน

จุดสำคัญบนเส้นลายนิ้วมือ (Minutiae)

ในลายนิ้วมือหนึ่งๆ จะประกอบด้วยจุดสำคัญบนเส้นลายนิ้วมือมากมายและลายนิ้วมือแต่ละอันที่มาจากต่างบุคคลหรือมาจากต่างนิ้วมือก็จะมีจุดสำคัญบนเส้นลายนิ้วมือที่แตกต่างกันไป โดยเอกลักษณ์หรือความแตกต่างจะพิจารณาจากจุดสำคัญบนเส้นลายนิ้วมือเป็นสำคัญ ได้แก่

1) Ridge ending (Termination) เป็นลักษณะที่เส้นลายนิ้วมือสิ้นสุดโดยทันทีทันใด

2) Bifurcation เป็นลักษณะที่เส้นลายนิ้วมือเดินทางมาจาก 1 เส้น แล้วแตกแยกออกเป็น 2 เส้นหรือมากกว่า 2 เส้น

3) Enclosure (Lake) เป็นลักษณะที่เส้นลายนิ้วมือเดินทางมาจาก 1 เส้น แล้วแยกออกและมารวมกันอีกครั้งจนเกิดเป็นพื้นที่ปิด

4) Independent ridge เป็นลักษณะที่เส้นลายนิ้วมืออยู่อย่างอิสระไม่เชื่อมต่อกับเส้นอื่น มีลักษณะค่อนข้างสั้น แต่ไม่สั้นจนถือว่าเป็น Ridge dot

5) Ridge dot (Point or island) เป็นลักษณะที่เส้นลายนิ้วมือสั้นมากจนสามารถเปรียบเทียบได้ว่าเป็นจุด

6) Spur เป็นลักษณะที่เส้นลายนิ้วมือ 1 เส้น มีเส้นลายนิ้วมืออีกเส้นแยกออกมาเพียงเล็กน้อย คล้ายกับลักษณะเดือยไก่

7) Crossover เป็นลักษณะที่เส้นลายนิ้วมือ 2 เส้นซึ่งวิ่งมาคู่กันมีเส้นลายนิ้วมือเล็กๆ แยกออกมาเชื่อมทั้งสองเส้นเข้าด้วยกัน

ที่กล่าวมาข้างต้นทำให้ทราบแนวนโยบายของมหาวิทยาลัยที่ให้ความสำคัญเรื่องการมาปฏิบัติงานของพนักงานและลูกจ้างด้วยการลงเวลาเข้างาน การออกงาน โดยการสแกนลายนิ้วมือเป็นอย่างมาก กล่าวได้ว่าการระบุตัวบุคคลที่ใช้ลักษณะเฉพาะของลายนิ้วมือเป็นที่เชื่อถือและยอมรับอย่างแพร่หลายมากขึ้น ด้วยเหตุที่ลายนิ้วมือ (Fingerprint) คือ ลายเส้นนูนที่ปรากฏอยู่บนผิวหนังด้านหน้าของนิ้วมือ ซึ่งจะแตกต่างกันในแต่ละบุคคล ถึงแม้จะเป็นแฝดที่เกิดจากไข่ฟองเดียวกันก็ตาม และจะไม่เปลี่ยนแปลงเลยตลอดชีวิต ลายนิ้วมือเป็นลักษณะพันธุกรรมที่มียีนหลายคู่และเริ่มก่อกำเนิดตั้งแต่เป็นทารกอยู่ในครรภ์มารดาช่วงอายุประมาณสัปดาห์ที่ 8 จนถึงประมาณสัปดาห์ที่ 25 จึงมีรูปแบบคงที่ไม่เปลี่ยนแปลงไปจนตลอดชีวิต (สมทรง ณ นคร และคณะ, 2554, น. 952) และเมื่อพบอุบัติเหตุกับลายนิ้วมือ ร่างกายเราก็จะซ่อมแซมส่วนที่สึกหรอเองได้ ดังนั้นลายนิ้วมือจึงถูกนำมาใช้ประโยชน์ในหลายด้านด้วยกัน เช่น การตรวจสอบลายพิมพ์นิ้วมือเพื่อพิสูจน์ตัวตนของบุคคล เพื่อตรวจหาเจ้าของลายนิ้วมือที่ใช้ในงานด้านอาชญากรรม การยืนยันตัวตนเพื่อผ่านเข้าออกอาคารหรือห้องนิรภัยด้วยลายนิ้วมือ เป็นต้น

ภาพที่ 3.9 แสดงรูปแบบของลายนิ้วมือ

3.2 วิธีการปฏิบัติงาน

เครื่องสแกนลายนิ้วมือแบบที่ใช้งานเป็นลักษณะเครื่องสแกนที่ใช้แสงเป็นหัวอ่าน มีการทำงานพื้นฐาน 2 อย่างที่จะต้องทำ คือ (1) ต้องการที่จะให้ภาพของนิ้วมือปรากฏขึ้น และ (2) ต้องการที่จะกำหนดทั้งรูปแบบของรอยสันนูนและรอยร่องลึกในภาพเพื่อให้ตรงกันกับรูปแบบของรอยสันนูนและรอยร่องลึกในภาพที่สแกนไว้ก่อนหน้านี้ ขั้นตอนของการใช้งานระบบสแกนลายนิ้วมือ ผู้ใช้ทุกคนในระบบจะต้องบันทึกลายนิ้วมือแม่แบบเข้าสู่ระบบผ่าน Sensor จัดเก็บแม่แบบลายนิ้วมือก่อน ส่วนจะเป็นการจัดเก็บแบบไหนนั้นขึ้นอยู่กับเทคโนโลยีที่เจ้าของผลิตภัณฑ์เครื่องสแกนลายนิ้วมือเลือกใช้ เช่น จัดเก็บเป็นรูปภาพ (Pattern) หรือจัดเก็บเป็นจุดตัดจุดไม่ต่อเนื่องบนลายนิ้วมือ (Minutiae) เป็นต้น เมื่อจัดเก็บข้อมูลลายนิ้วมือผู้ใช้ผ่าน Sensor แล้ว ข้อมูลต้นแบบดังกล่าวจะถูกเข้ารหัสเพื่อความปลอดภัยไม่ให้มีการขโมยข้อมูลหรือคัดลอกข้อมูลเอาไปใช้ผิดวัตถุประสงค์ เมื่อต้องการตรวจพิสูจน์ลายนิ้วมือของบุคคล เครื่องจะทำการวิเคราะห์เปรียบเทียบข้อมูลลายนิ้วมือของผู้ที่ต้องการตรวจสอบกับลายนิ้วมือต้นแบบที่อยู่ในฐานข้อมูลระบบทั้งหมด

ภาพที่ 3.10 อุปกรณ์เก็บลายนิ้วมือ

กระบวนการตรวจพิสูจน์บุคคลด้วยระบบ Biometrics จะมีขั้นตอนมาตรฐานเหมือนกัน ดังนี้

1) ผู้ใช้ระบบจะต้องให้ตัวอย่าง (Samples) ของลักษณะทางระบบ Biometrics ที่จะใช้หรือเรียกว่าเป็นการลงทะเบียนไว้ในระบบ ซึ่งกำหนดให้เก็บลายนิ้วมือที่เป็นนิ้วชี้ขวา, นิ้วชี้ซ้าย

ภาพที่ 3.11 การลงทะเบียนเก็บลายนิ้วมือ

2) ตัวอย่างทาง Biometrics ที่ถูกเก็บไว้ในขั้นตอนแรก จะถูกเก็บไว้เป็น Template เพื่อรอการเปรียบเทียบ ขั้นตอนที่ (1) และขั้นตอนที่ (2) เรียกรวมกันว่าการ Enrollment ซึ่งจะทำเพียงครั้งแรกครั้งเดียวเท่านั้น

3) เมื่อผู้ใช้ต้องการเปรียบเทียบ จะทำการเก็บตัวอย่าง Biometrics ของผู้ใช้อีกครั้งเพื่อนำไปเปรียบเทียบกับ Template ที่เก็บไว้แล้วก่อนที่จะวิเคราะห์และประมวลผลเพื่อจะยอมรับ หรือ ปฏิเสธ ขั้นตอนนี้เรียกว่า กระบวนการตรวจสอบสิทธิ์ใช้งาน (Authentication) หรือตรวจสอบผู้ใช้ (Identification) ผลของการตรวจสอบผู้ใช้ในขั้นตอนที่ (3) เป็นได้ 2 กรณี คือ

- Correct Accept: อนุญาตให้ผู้ใช้มีสิทธิ์ผ่านเข้าสู่ระบบ
- Correct Reject: ปฏิเสธการใช้งานผู้ใช้ที่ไม่มีสิทธิ์ผ่านเข้าสู่ระบบ

ประเภทเครื่องสแกนลายนิ้วมือของมหาวิทยาลัยวลัยลักษณ์ที่ใช้งานอยู่มี 2 รุ่น ดังนี้

(1) เครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800 มีคุณสมบัติ

1) มีหน่วยความจำรองรับลายนิ้วมือผู้ใช้ได้ 8,000 คน

2) จัดเก็บ log ข้อมูลการใช้งานได้ 200,000 รายการ

3) ใช้หัวอ่านแบบแสงที่มีความแข็งแกร่งทนทานต่อการขีดข่วนด้วยของแข็ง ของมีคม การสั่นสะเทือน ไฟฟ้าสถิตย์

4) มีฝาครอบเลนส์สแกน ป้องกันฝุ่นละออง น้ำ แสง

5) ตัวเครื่องจะมีกล้องถ่ายรูป (ID Camera) จับภาพผู้ใช้ขณะสแกนลายนิ้วมือ

6) หน้าจอขนาด 3.5" แสดงภาพถ่ายผู้ใช้

7) Built-in Battery Backup สามารถทำงานใน Mode Mobile ได้ 3-4 ชั่วโมง (Recharge ได้)

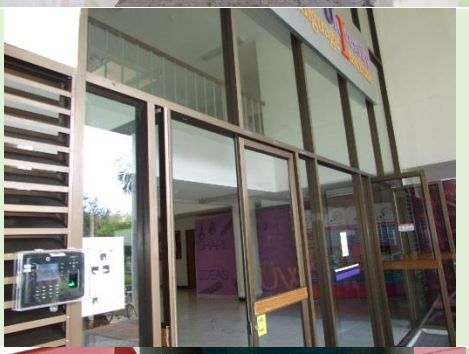
ภาพที่ 3.12 MATCHER รุ่น M-800

ตารางที่ 3.3 แสดงตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
1	อาคารบรรณสารและสื่อการศึกษา ชั้น 1 ด้านทางเข้าหลัก	
2	อาคารคอมพิวเตอร์ ชั้น 1 ด้านหน้าอาคาร	

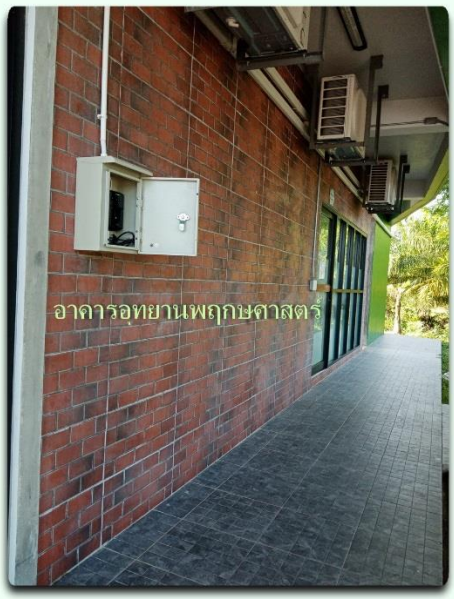
No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
3	อาคารไทยบุรี ชั้น 2 ศูนย์บริการการศึกษา	
4	อาคารเครื่องมือวิทยาศาสตร์และเทคโนโลยี 8 ชั้น 1	
5	อาคารเครื่องมือวิทยาศาสตร์และเทคโนโลยี 5 (ฝ่ายบริการและใช้ประโยชน์เครื่องมือ)	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
6	อาคารเครื่องมือวิทยาศาสตร์และเทคโนโลยี 5 ชั้น 1 ด้านหน้าอาคาร	
7	อาคารบริหาร ประตูทางเข้า ชั้น 1 ส่วนพัสดุ	
8	อาคารบริหาร ส่วนทรัพยากรมนุษย์และองค์กร	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
9	อาคารวิชาการ 9 ด้านข้างโรงจอดรถ	
10	อาคารวิชาการ 5 ด้านหน้าทางเข้าของอาคาร	
11	อาคารวิชาการ 4 ด้านข้างโรงจอดรถ	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
12	อาคารวิชาการ 3 ด้านข้างโรงจอดรถ	
13	อาคารวิชาการ 2 ด้านข้างโรงจอดรถ	
14	อาคารวิชาการ 1 ด้านข้างโรงจอดรถ ใกล้กับอาคารวิจัย	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
15	อาคารวิจัย ชั้น 1 ด้านหน้าอาคาร	
16	อาคารปฏิบัติการเทคโนโลยีและพัฒนานวัตกรรม	
17	อาคารสโมสร ชั้น 1	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
18	อาคารวิทยาการสุขภาพ	
19	อาคารสหกิจศึกษา	
20	อาคารอุทยานพฤกษศาสตร์	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ MATCHER รุ่น M-800	ภาพถ่ายจากสถานที่จริง
21	อาคารอายุกรรมและศัลยกรรมม้าและโค	

(2) เครื่องสแกนลายนิ้วมือ รุ่น Standalone มีคุณสมบัติ

1) มีหน่วยความจำรองรับลายนิ้วมือผู้ใช้ได้ 800 คน

2) จัดเก็บ log ข้อมูลการใช้งานได้ 20,000 รายการ

3) เลนส์ที่ใช้ในการสแกนเป็นประเภท OPTICAL มีความละเอียดที่ 500 dpi

4) เลนส์ที่ใช้สามารถสแกนได้ในลักษณะ 360 องศา

5) ใช้เวลาในการสแกนลายนิ้วมือไม่เกิน 3 วินาที

6) ตัวเครื่องมีปุ่ม IN บอกสถานะในการสแกนลายนิ้วมือเพื่อบันทึกเวลาเข้างาน และ ปุ่ม OUT บอกสถานะในการสแกนลายนิ้วมือเพื่อบันทึกเวลาออกงาน

7) ตัวเครื่องมีไฟบอกสถานะในการสแกนลายนิ้วมือเมื่อบันทึกเวลาเข้า-ออกงาน ในลักษณะสถานะไฟเขียวแสดงว่า Pass ส่วนสถานะไฟแดงแสดงว่า Fail

ภาพที่ 3.13 เครื่องสแกนลายนิ้วมือ รุ่น Standalone

ตารางที่ 3.4 แสดงตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone	ภาพถ่ายจากสถานที่จริง
1	อาคารเครื่องมือวิทยาศาสตร์และเทคโนโลยี 5 ชั้น 1 ด้านใน	
2	อาคารส่วนอาคารสถานที่ ชั้น 1	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone	ภาพถ่ายจากสถานที่จริง
3	อาคารศูนย์การแพทย์ (D) ชั้น G	
4	อาคารวิชาการ 8 งานธุรการ	
5	อาคารวิชาการ 7 งานธุรการ	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone	ภาพถ่ายจากสถานที่จริง
6	อาคารวิชาการ 6 งานห้อง Lab สำนักสารสนเทศศาสตร์	
7	อาคารสถาปัตยกรรมศาสตร์และการออกแบบ	
8	อาคารวิจัย ชั้น 1 ด้านในอาคาร	
9	อาคารกิจกรรมนักศึกษา ที่ปรึกษาห้องพัก	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone	ภาพถ่ายจากสถานที่จริง
10	อาคารโรงประปา งานธุรการ	
11	อาคารวิทยาศาสตร์การกีฬา งานธุรการ	

No	ตำแหน่งที่ติดตั้งเครื่องสแกนลายนิ้วมือ รุ่น Standalone	ภาพถ่ายจากสถานที่จริง
12	อาคารฟาร์ม	
13	อาคาร PC Tower ชั้น 9 งานธุรการ จ.สุราษฎร์	
14	อาคาร SM ชั้น 19 งานธุรการ กทม.	

3.3 เงื่อนไข/ข้อสังเกต/ข้อควรระวัง/สิ่งที่ควรคำนึงในการปฏิบัติงาน

1) การลงทะเบียนเก็บบันทึกลายนิ้วมือแม่แบบ (Enrollment) เข้าสู่ระบบโดยการใช้โปรแกรมเก็บลายนิ้วมือของพนักงานที่เข้าใหม่นั้น ต้องคำนึงถึงการวางนิ้วมือของพนักงานใหม่ในตำแหน่งตรงกลางของเลนส์ และขอเป็นนิ้วชี้ขวา-ซ้าย ซึ่งควรได้รายละเอียดของภาพที่มีคุณภาพดีมากถึงมากที่สุด มิฉะนั้นจะเกิดปัญหาการไปใช้งานของพนักงาน
2) กรณีที่เก็บลายมือนิ้วชี้ขวา-ซ้าย ที่ไม่ได้ในระดับคุณภาพดีมากถึงมากที่สุด ให้เลื่อนมาเก็บที่นิ้วมือหัวแม่โป้งขวา-ซ้าย แทน
3) เมื่อผ่านขั้นตอนการ Enrollment แล้ว ต้องทำการกำหนดสิทธิ์ให้กับพนักงานใหม่แล้วส่งสิทธิ์ดังกล่าวไปยังจุดใช้งานตามที่กำหนดไว้ให้สำเร็จ
4) ควรตรวจสอบสิทธิ์ดังกล่าวของพนักงานใหม่จากโปรแกรม ซึ่งต้องปรากฏข้อมูลของพนักงานใหม่ไปยังเครื่องสแกนลายนิ้วมือจุดใช้งานด้วย

3.4 แนวคิด/งานวิจัยที่เกี่ยวข้อง

คู่มือการปฏิบัติงานระบบสแกนลายนิ้วมือ เป็นคู่มือสำหรับผู้ปฏิบัติงานในฐานะ Admin ด้านการใช้งานระบบสแกนลายนิ้วมือ โดยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องมาประกอบและใช้เป็นแนวทางในการจัดทำเพื่อให้สามารถทำงานได้อย่างดีมีมาตรฐานและคุณภาพ ดังนี้

ปัจจุบันการตรวจสอบพิสูจน์และยืนยันตัวตนของบุคคล มีความสำคัญทั้งด้านการแพทย์ การสำรวจประชากร อาชญากรรม ความมั่นคงของประเทศ จึงจำเป็นต้องหาวิธีการที่มีความถูกต้อง แม่นยำสูง ที่เหมาะสมและเป็นที่น่าเชื่อถือ วิธีการลักษณะนี้เป็นการพิสูจน์และระบุตัวตนโดยใช้เทคโนโลยีชีวมิติ (Biometric Technology) อาศัยข้อมูลทางกายภาพที่มีความเป็นเอกลักษณ์ของบุคคลที่ไม่ซ้ำกับใคร นั่นคือ ลายนิ้วมือ (สำรวน เวียงสมุทร, 2554) ด้วยลักษณะพื้นฐานของลายนิ้วมือที่มีความแตกต่างของแต่ละบุคคล ประกอบกับความคงอยู่ถาวร ไม่สามารถปลอมแปลงได้ การระบุหรือแสดงตัวตนที่ให้ความแม่นยำและรวดเร็ว เป็นที่ยอมรับ ส่งผลให้หน่วยงาน องค์กรภาครัฐ เอกชน นำมาประยุกต์ใช้งานได้จริง ได้แก่

- งานธุรกรรมทางการเงินของธนาคารแห่งประเทศไทย ออกประกาศที่ ธปท.ฝทง. ว.760/2563 เรื่อง นำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน ลงวันที่ 22 กรกฎาคม 2563 โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้บริการทางการเงินที่มีการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงิน ใช้อ้างอิงเป็นมาตรฐานเพื่อให้มั่นใจว่าการให้บริการที่เกี่ยวข้องกับเทคโนโลยีชีวมิติมีความมั่นคงปลอดภัย สอดคล้องกับมาตรฐานสากล ซึ่งจะช่วยยกระดับการให้บริการทางการเงินและก่อให้เกิดประโยชน์แก่ผู้ใช้บริการ (ธนาคารแห่งประเทศไทย, 2563)

- งานด้านการลงเวลาการเข้าเรียนจริงด้วยลายนิ้วมือ โดยนักศึกษาคณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมไฟฟ้า มหาวิทยาลัยบูรพา พบว่าที่ผ่านมาอาจารย์ผู้สอนต้องทำการเช็คชื่อผู้เรียนในห้องเรียน บางครั้งขานชื่อเรียกได้ยินบ้าง ไม่ได้ยินบ้าง และค่อนข้างเสียเวลาในการกระทำดังกล่าว จึงคิดพัฒนาระบบตรวจสอบการเข้าเรียนแบบเวลาจริงด้วยลายนิ้วมือ (พลากร ป้องกัน และ วีรวัฒน์ บุญโต, 2561) โดยผ่านสัญญาณ WiFi พร้อมแสดงผลการเข้าเรียนบนเว็บได้ถูกต้องและรวดเร็วในอัตราเฉลี่ย 3.62 วินาทีต่อคน

- งานด้านการยืม-คืนหนังสือด้วยเครื่องสแกนลายนิ้วมือของสำนักหอสมุด มหาวิทยาลัยทักษิณ นำเทคโนโลยีชีวมิติ โดยใช้ลายนิ้วมือของบุคคลในการระบุตัวตนของผู้ใช้บริการของหอสมุด (พิทย์พิมล ชูรอด เนาวลักษณ์ แสงสนิท และ สุพิริยา ผลนาค, 2557) เพื่อลดปัญหาการใช้บัตรของผู้อื่นมายืมหนังสือ ผลทำให้มีความปลอดภัยและน่าเชื่อถือของระบบยืม-คืนหนังสือมากยิ่งขึ้น

- งานด้านการรักษาความปลอดภัยภายในองค์กรโดยการสแกนลายนิ้วมือ โดยนักศึกษาสำนักวิชาวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีสุรนารี เห็นว่าความปลอดภัยในองค์กรถือเป็นความสำคัญ ซึ่งสถาบันการศึกษาควรมีวิธีการการระบุตัวตนของผู้ที่มีสิทธิ์การผ่านเข้าประตูที่สำคัญของหน่วยงาน จึงเลือกทำโครงงานเครื่องสแกนลายนิ้วมือเพื่อเปิด-ปิดประตู (อรรถพล ศิลปะกิจโกศล, ชาญณรงค์ ประกอบดี และ ภูริทัต สุธรรมมา, 2553) ผลการจัดทำ พบว่า ประตูจะเปิดให้กับบุคคลที่มีข้อมูลลายนิ้วมือที่อยู่ในระบบเท่านั้น และระบบทำงานด้วยการใช้เครื่องรับ–ส่งสัญญาณ ผ่านพอร์ต RS-232 แบบไร้สาย ที่มีประสิทธิภาพและลดต้นทุนในการติดตั้งระบบ

- งานด้านการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตามมาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ เกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (DIGITALIZATION: DIGITAL ID - IDENTITY PROOFING AND AUTHENTICATION) เวอร์ชัน 1.0 (สำนักงานพัฒนารัฐบาลดิจิทัล สำนักนายกรัฐมนตรี, 2564) เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยพัฒนาตามแนวมาตรฐานของ (1) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน และ (2) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน การพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นกระบวนแรกที่สำคัญในการเข้าสู่บริการภาครัฐ โดยมีข้อกำหนดที่ 2.4.1 วิธีการพิสูจน์และยืนยันตัวตนแบบพบเห็นต่อหน้า หัวข้อย่อยที่ (6) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ (biometric comparison) เช่น ภาพใบหน้า หรือ ลายนิ้วมือ ต้องตรวจสอบเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตนว่าตรงกับผู้สมัครใช้บริการรายนั้นจริง จึงจะให้รับบริการในครั้งนั้นได้

ตัวอย่างการประยุกต์ใช้งานที่กล่าวมาแล้วนั้นเห็นผลว่าการใช้ลายนิ้วมือเพื่อการพิสูจน์และยืนยันตัวตนสามารถใช้ประโยชน์ได้ในหลายด้านอย่างถูกต้องและเป็นจริง ปัจจุบันมีการนำแนวคิดการลงเวลา

ปฏิบัติงานเพื่อแสดงสถานะการเข้างานและการออกงานในอาคารที่ทำงานด้วยการใช้แอปพลิเคชันบนสมาร์ตโฟนแล้วโดยใช้เวลาเพียง 1 วินาทีต่อการลงเวลา ในส่วนขั้นตอนดำเนินงานของการประยุกต์ใช้งานระบบสแกนลายนิ้วมือในมหาวิทยาลัยวลัยลักษณ์ จะขอกล่าวถึงในบทที่ 4 เป็นลำดับถัดไป

บทที่ 4
เป้าหมายและเทคนิคในการปฏิบัติงานแบบมุ่งผลสัมฤทธิ์

บทนี้ เป็นการอธิบายเกี่ยวกับเป้าหมายในการปฏิบัติงาน เทคนิคในการวางแผน/แผนกลยุทธ์ในการปฏิบัติงาน เทคนิคในการปฏิบัติงานแต่ละขั้นตอนการปฏิบัติงาน เทคนิคการทำให้ผู้รับบริการพึงพอใจ และจรรยาบรรณ/ คุณธรรม/จริยธรรมในการปฏิบัติงาน

4.1 เป้าหมายในการปฏิบัติงาน (ตัวชี้วัดในการปฏิบัติงาน)

เป้าหมายในการปฏิบัติงานระบบงานสแกนลายนิ้วมือเพื่อให้ผู้ปฏิบัติงานสามารถทำงานแทนกันได้ และการปฏิบัติงานเป็นมาตรฐานเดียวกัน จึงต้องกำหนดขั้นตอนการทำงานดังต่อไปนี้

ลำดับ	รายการ	ตัวชี้วัด (KPI)	
		เชิงปริมาณ	เชิงคุณภาพ
1	ได้รับแจ้งผ่านเมลถึงจำนวนการจัดเก็บลายนิ้วมือพนักงานใหม่ จากส่วนทรัพยากรมนุษย์และองค์กร	- จำนวนคน	
2	ตรวจสอบข้อมูลพนักงานใหม่ว่าถูกต้อง ประกอบด้วย รหัส คำนำหน้าชื่อ-สกุล ตำแหน่ง สังกัด		- 100 %
3	ยืนยันว่าข้อมูลพนักงานใหม่ที่แจ้งมามีความถูกต้อง		- 100 %
4	หากข้อมูลพนักงานใหม่ที่แจ้งมาไม่ความถูกต้อง ปรับแก้ไขทันที		- ทันเวลา
5	ข้อมูลพนักงานใหม่ที่ถูกต้องตรงกันจะถูกนำไปใช้งานในฐานข้อมูล Oracle		- พร้อมใช้งาน

4.2 เทคนิคในการวางแผน/แผนกลยุทธ์ในการปฏิบัติงาน

เมื่อข้อมูลพนักงานใหม่ที่ถูกต้องตรงกันพร้อมให้นำไปใช้งานในฐานข้อมูล Oracle งานระบบสแกนลายนิ้วมือก็เริ่มทำงานด้วยแผนปฏิบัติการดังตารางที่ 4.1

ตารางที่ 4.1 แผนปฏิบัติการงานระบบสแกนลายนิ้วมือ (Finger Scan)

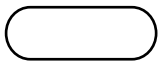
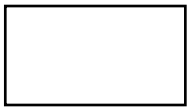
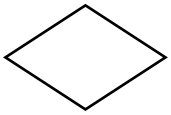
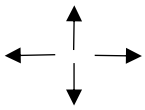
ผู้รับผิดชอบ	กิจกรรม	ระยะเวลาดำเนินการ
วลัยพร เนียมเล็ก (ส่วนทรัพยากรมนุษย์และองค์กร)	**1) นำเข้าข้อมูลพนักงานใหม่**	**5 นาที**
ประไพศรี เหล่าทองมีสกุล (ศูนย์เทคโนโลยีดิจิทัล)	**2) ตรวจสอบพร้อมปรับแก้ข้อมูลให้ถูกต้อง**	**1 นาที**
ประไพศรี เหล่าทองมีสกุล (ศูนย์เทคโนโลยีดิจิทัล)	**3) กำหนดสิทธิ์ให้กับพนักงานใหม่**	**1 นาที**
ประไพศรี เหล่าทองมีสกุล (ศูนย์เทคโนโลยีดิจิทัล)	**4) ส่งข้อมูลสิทธิ์ให้กับพนักงานใหม่**	**1 นาที**
ประไพศรี เหล่าทองมีสกุล (ศูนย์เทคโนโลยีดิจิทัล)	**5) ผลการทดสอบการใช้งาน**	**1 นาที**
ประไพศรี เหล่าทองมีสกุล (ศูนย์เทคโนโลยีดิจิทัล)	**6) นำเข้าข้อมูลการลงเวลาปฏิบัติงาน**	**8 นาที**
ประไพศรี เหล่าทองมีสกุล (ศูนย์เทคโนโลยีดิจิทัล)	**7) รายงานการลงเวลาปฏิบัติงาน**	**1 นาที**

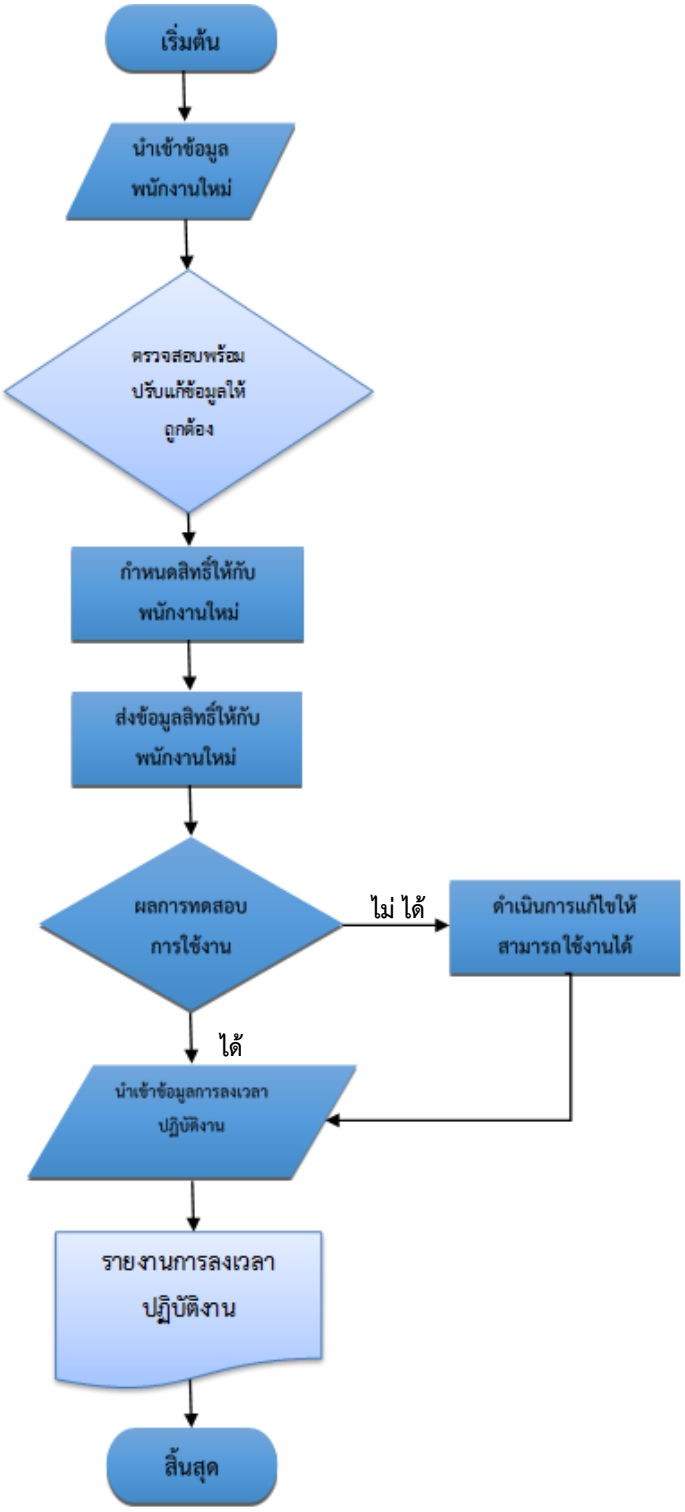
4.3 เทคนิคในการปฏิบัติงานแต่ละขั้นตอนการปฏิบัติงาน

ระบบสแกนลายนิ้วมือ (Finger Scan) นำโปรแกรมบริหารจัดการ Stand Alone Product Management 3.0 ซึ่งเป็นซอฟต์แวร์ที่ทำงานกับฐานข้อมูล Oracle เพื่อใช้ในการบริหารจัดการเกี่ยวกับการจัดเก็บข้อมูลลายนิ้วมือ ข้อมูลสิทธิ์การใช้งานเพื่อการลงเวลาปฏิบัติงานในอาคารที่ติดตั้งรวมทั้งสิ้น 35 จุด

สำหรับการปฏิบัติงานในกระบวนการปฏิบัติงานระบบสแกนลายนิ้วมือ เพื่ออำนวยความสะดวกให้ผู้ปฏิบัติงานได้เข้าใจลำดับขั้นตอนการทำงานที่ครบวงจร โดยมีสัญลักษณ์ ชื่อเรียก และความหมายของ Flow chart (ตารางที่ 4.2) มีขั้นตอนการปฏิบัติงาน (ภาพที่ 4.1)

ตารางที่ 4.2 สัญลักษณ์ ชื่อเรียก และความหมายของ Flow chart

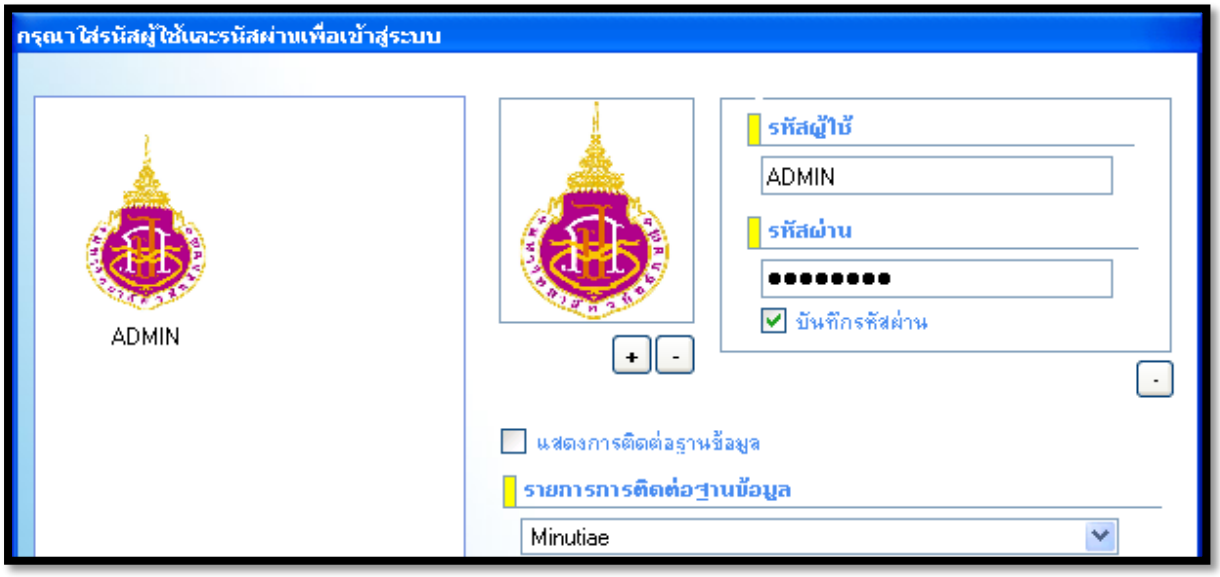
สัญลักษณ์	**ชื่อเรียก**	**ความหมายของ Flow chart**
	เริ่มต้น/สิ้นสุด	จุดเริ่มต้นและจุดสิ้นสุดของผังงาน
	การปฏิบัติงาน	จุดที่มีการปฏิบัติงานอย่างใดอย่างหนึ่ง
	การตัดสินใจ	จุดที่ต้องเลือกปฏิบัติงานอย่างใดอย่างหนึ่ง
	เอกสาร	พิมพ์ออกมาเป็นรายงานเอกสาร
	ทิศทาง	ทิศทางของขั้นตอนการดำเนินงาน
	รับข้อมูล	รับข้อมูล หรือ นำเข้าข้อมูล



ภาพที่ 4.1 ขั้นตอนการปฏิบัติงาน : เมื่อมีพนักงานใหม่เข้ามาทำงาน

การนำเครื่องสแกนลายนิ้วมือมาใช้งานในมหาวิทยาลัยเพื่อลงเวลาปฏิบัติงานของพนักงานและลูกจ้างสายปฏิบัติการวิชาชีพและบริหารทั่วไป ลักษณะงานจะเริ่มจากการมารายงานตัวของพนักงานเพื่อขึ้นทะเบียนประวัติพนักงานที่ส่วนทรัพยากรมนุษย์และองค์กร ขั้นตอนการทำงานเกิดขึ้นดังนี้

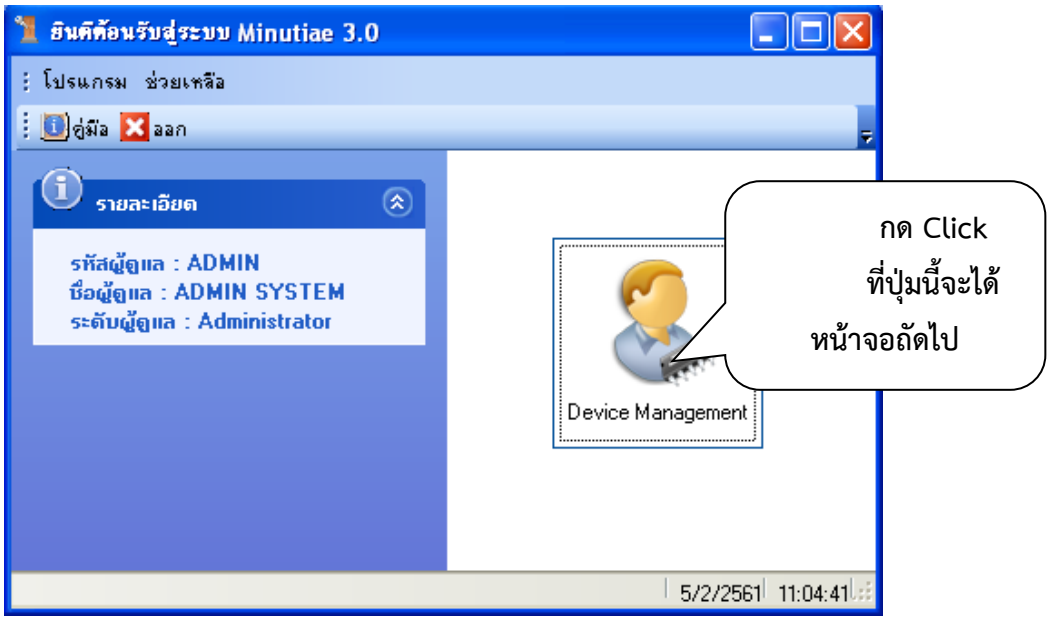
1) นำเข้าข้อมูลพนักงานใหม่ ข้อมูลที่ประกอบด้วย รหัส ชื่อ-นามสกุล เพศ หน่วยงานที่สังกัด วัน-เดือน-ปี ที่เริ่มทำงาน จะถูกนำเข้าสู่ฐานข้อมูล Oracle ชื่อ “FING” โดยโปรแกรมบริหารจัดการ Stand Alone Product Management 3.0



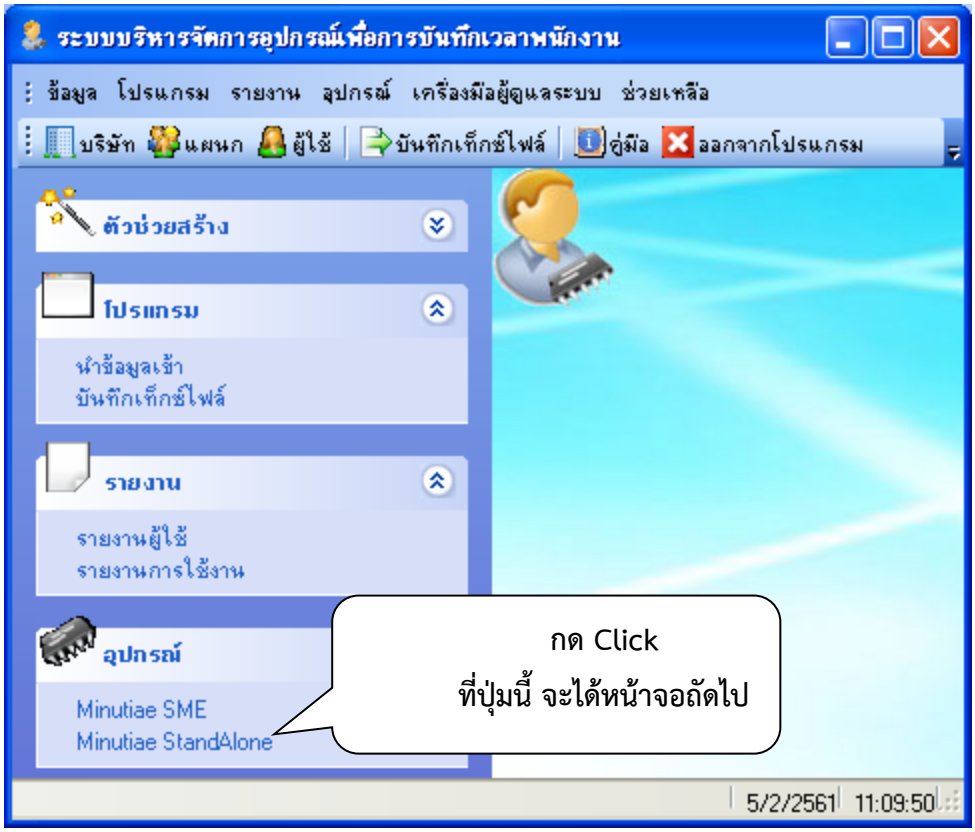
ภาพที่ 4.2 หน้าจอโปรแกรมบริหารจัดการ Stand Alone Product Management 3.0

2) ตรวจสอบพร้อมปรับแก้ข้อมูลให้ถูกต้อง ดำเนินการตรวจสอบข้อมูลเบื้องต้นจากการส่ง e-mail ที่มาจากส่วนทรัพยากรมนุษย์และองค์กร หากพบว่าข้อมูลที่ส่งมากับข้อมูลในฐานข้อมูลหลักไม่ตรงกัน ให้ปรับแก้ข้อมูลทุกฟิลด์ให้ถูกต้อง

3) กำหนดสิทธิ์ให้กับพนักงานใหม่ การกำหนดสิทธิ์ให้กับพนักงานใหม่ ในคู่มือนี้ ใช้ข้อมูลพนักงานใหม่นายสมมุติ ชื่อ นายอรรถพล กลยนี ตำแหน่ง นักวิชาการ สังกัด สำนักวิชาแพทยศาสตร์ เป็นข้อมูลตัวอย่าง โดยเริ่มแรกคือเข้าสู่โปรแกรมบริหารจัดการ Stand Alone Product Management 3.0 โดย User “ADMIN” และใส่รหัสผ่าน จะได้หน้าจอ



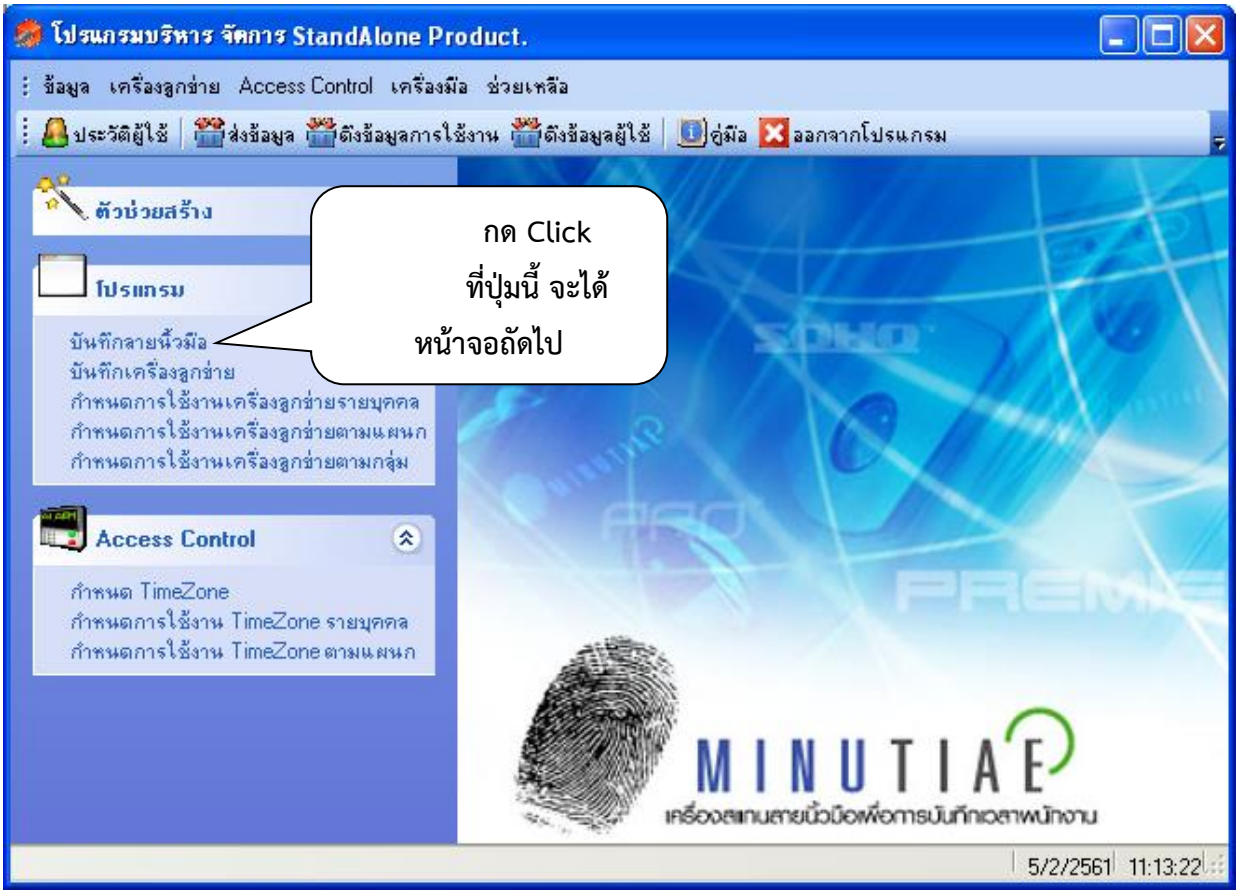
ภาพที่ 4.3 หน้าจอเกี่ยวกับ Device Management

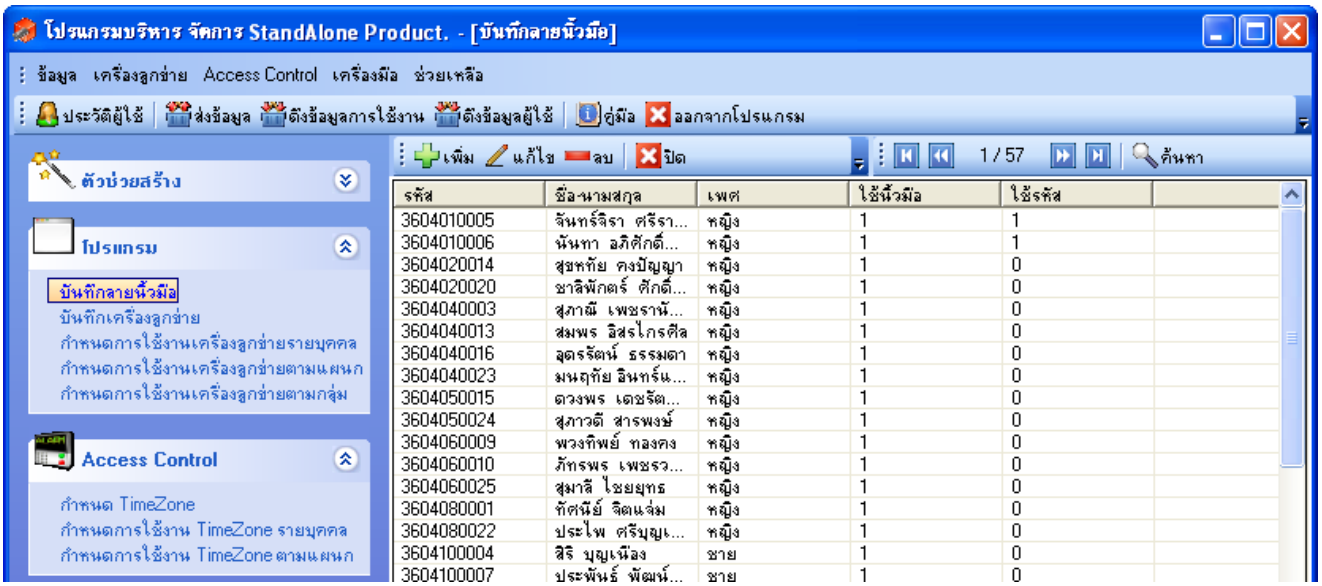


ภาพที่ 4.4 หน้าจอเกี่ยวกับระบบบริหารจัดการอุปกรณ์เพื่อการบันทึกเวลาพนักงาน

ภาพที่ 4.5 หน้าจอเกี่ยวกับโปรแกรมบริหารจัดการ Stand Alone Product

เริ่มดำเนินการที่แถบโปรแกรม “บันทึกลายนิ้วมือ” โดยการกด Click 1 ครั้ง



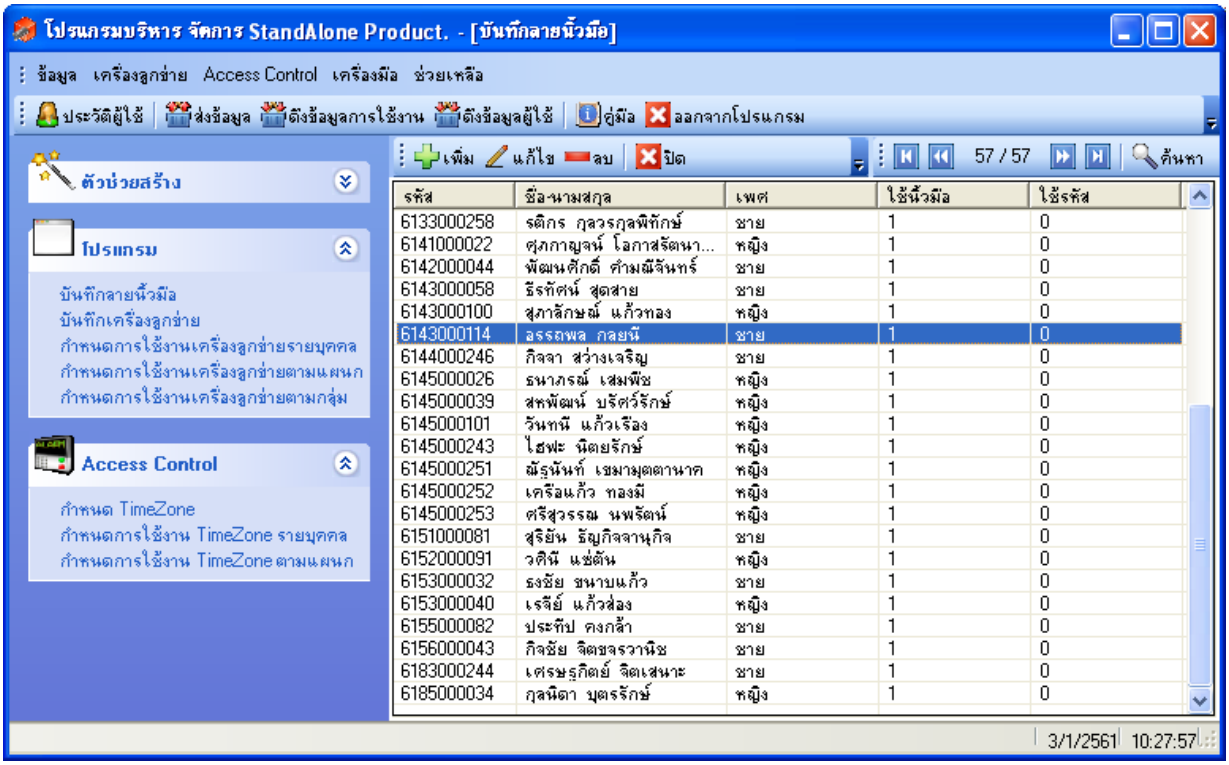


ภาพที่ 4.6 หน้าจอเกี่ยวกับโปรแกรมบริหารจัดการ Stand Alone Product [บันทึกลายนิ้วมือ]

ได้เมนูที่เห็นรายละเอียดของพนักงาน ให้ทำการค้นหา โดยใช้ปุ่ม  ใส่ชื่อ “อรรถพล” กดปุ่มตกลง

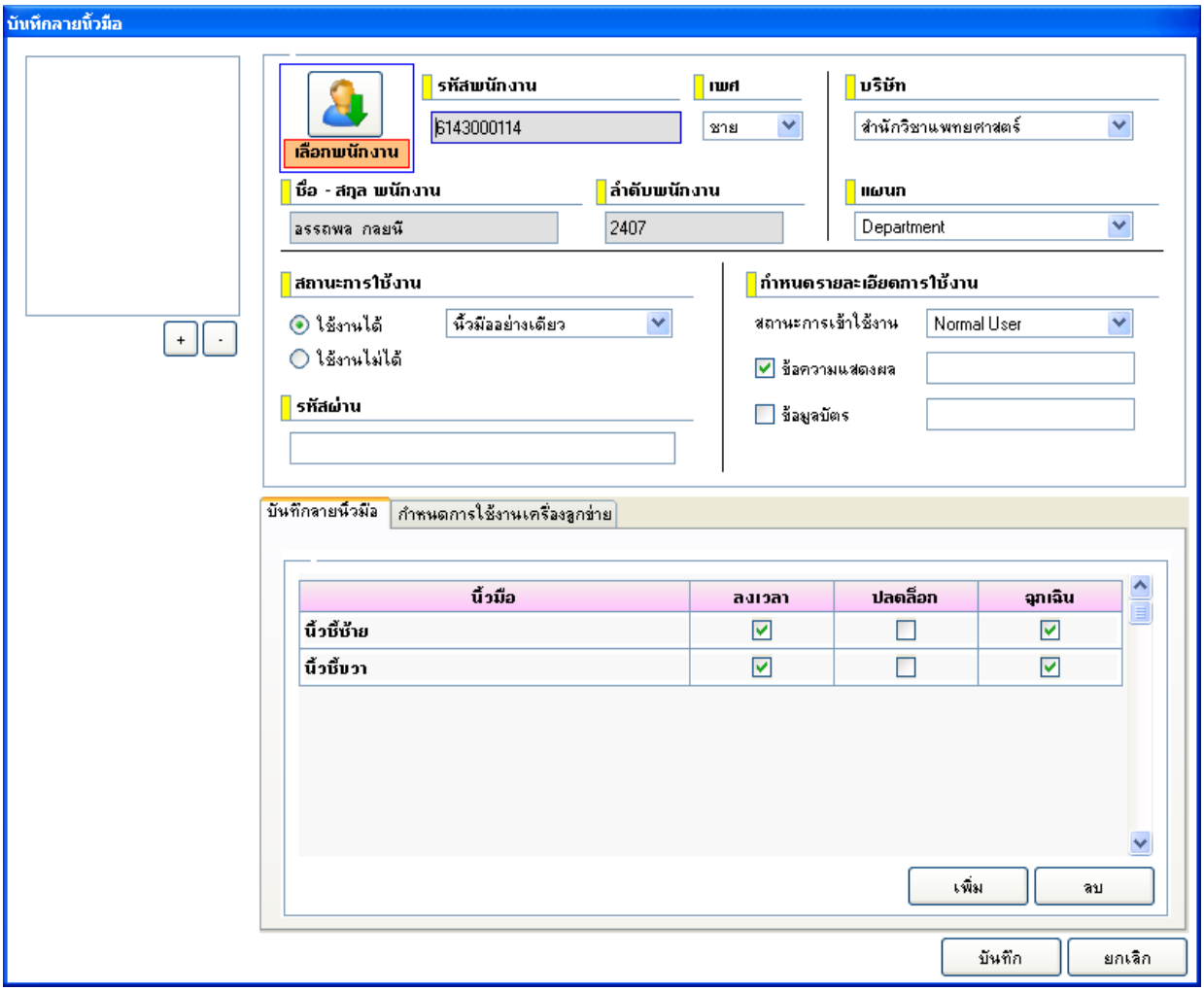
ภาพที่ 4.7 หน้าจอเกี่ยวกับค้นหาพนักงาน

จะปรากฏข้อมูลพนักงานที่ทำการค้นหา



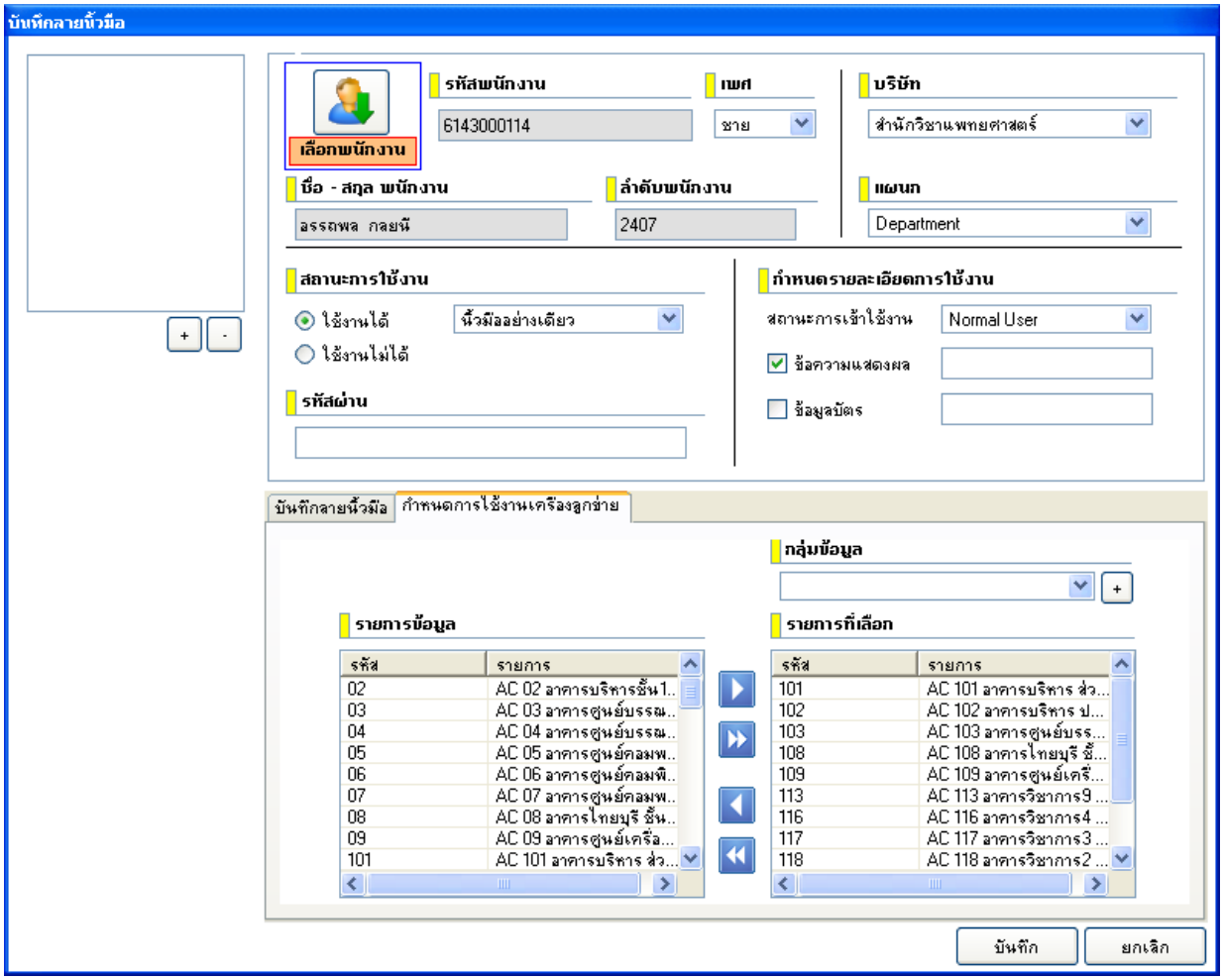
ภาพที่ 4.8 หน้าจอเกี่ยวกับผลการค้นหาพนักงาน

เมื่อทำการกด double Click ที่ชื่อ อรรถพล กลยนี ได้หน้าจอที่มีรายละเอียดของพนักงานท่านนี้



ภาพที่ 4.9 หน้าจอเกี่ยวกับรายละเอียดของพนักงาน “อรรถพล”

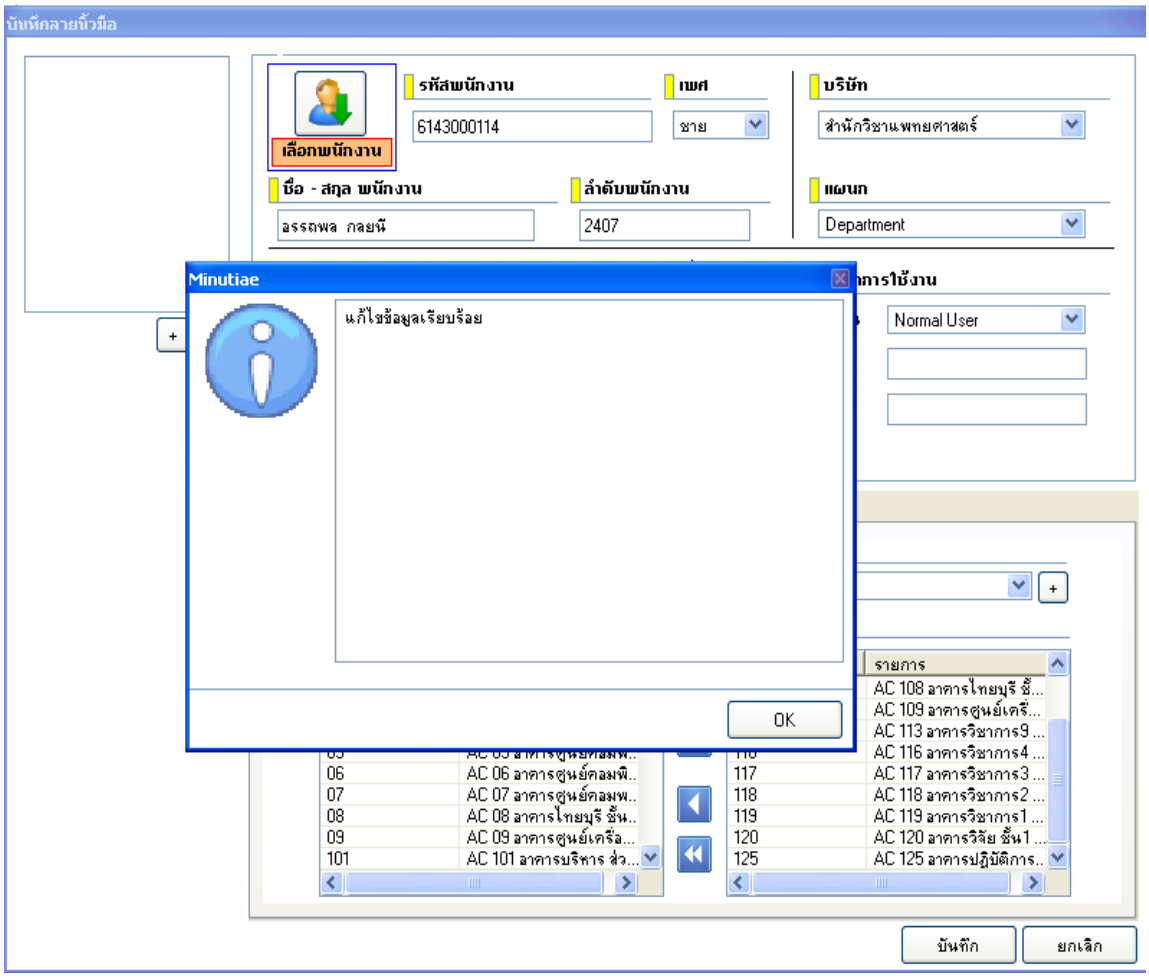
เลื่อนเมาส์ ไปที่แถบ “กำหนดการใช้งานเครื่องลูกข่าย” เพื่อทำการกำหนดสิทธิ์เครื่องลูกข่ายที่ให้ใช้งานเพื่อการสแกนลายนิ้วมือ ได้แก่จุดลงเวลาที่อาคารบริหาร อาคารบรรณสารและสื่อการศึกษา อาคารไทยบุรี อาคารวิชาการ 9-4-3-2-1 อาคารวิจัย และ อาคารปฏิบัติการเทคโนโลยีและนวัตกรรม



ภาพที่ 4.10 หน้าจอเกี่ยวกับรายละเอียดกำหนดการใช้งานเครื่องลูกข่ายของ “อรรถพล”

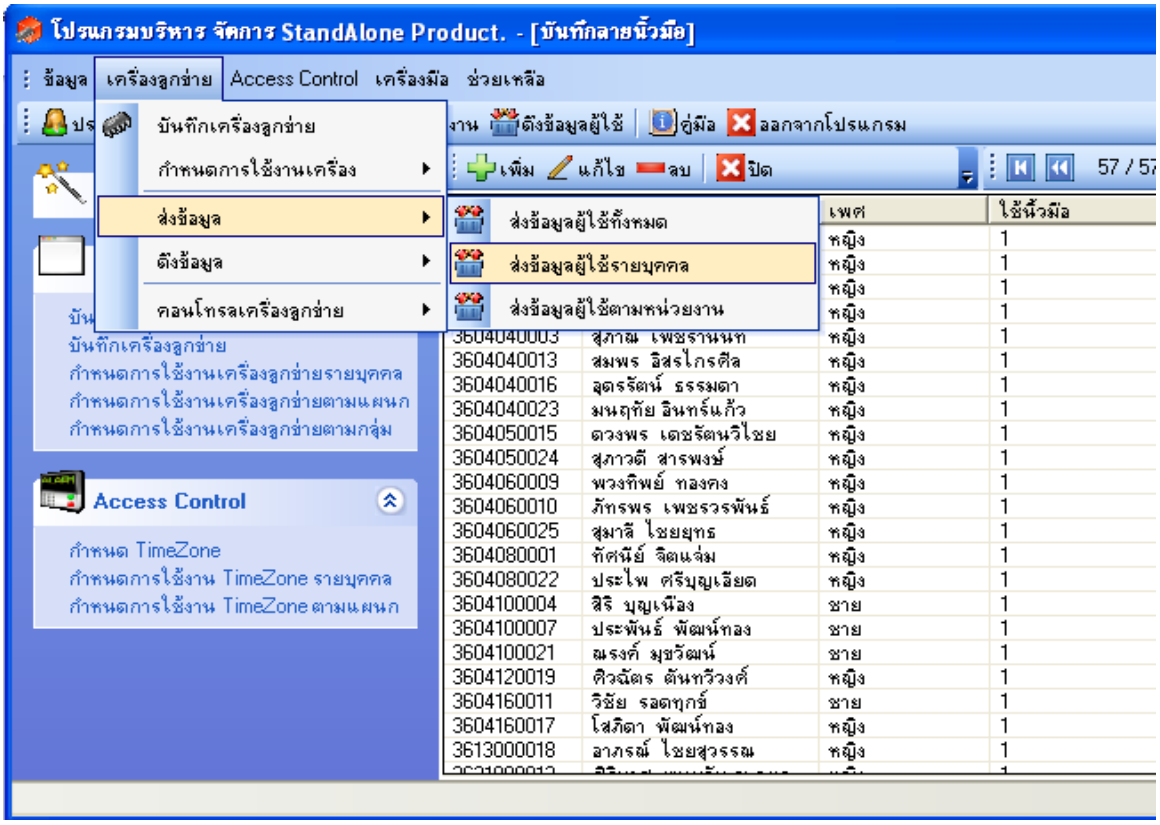
ให้ทำการบันทึกโดยกดปุ่ม “บันทึก”

เมื่อทำการกดปุ่มบันทึก จะได้หน้าจอนี้



ภาพที่ 4.11 หน้าจอเกี่ยวกับผลการบันทึกสำเร็จที่กำหนดการใช้งานเครื่องลูกข่าย ของ “อรรถพล”

4) ส่งข้อมูลสิทธิ์ให้กับพนักงานใหม่ ไปที่เมนูเครื่องลูกข่ายเลือก ส่งข้อมูล แบบ “ส่งข้อมูลผู้ใช้รายบุคคล”

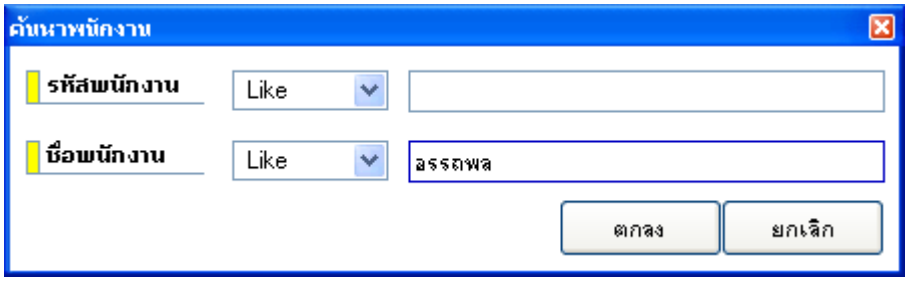


ภาพที่ 4.12 หน้าจอเกี่ยวกับการส่งข้อมูลผู้ใช้รายบุคคล

ไปที่ปุ่มค้นหา  กด Click 1 ครั้ง

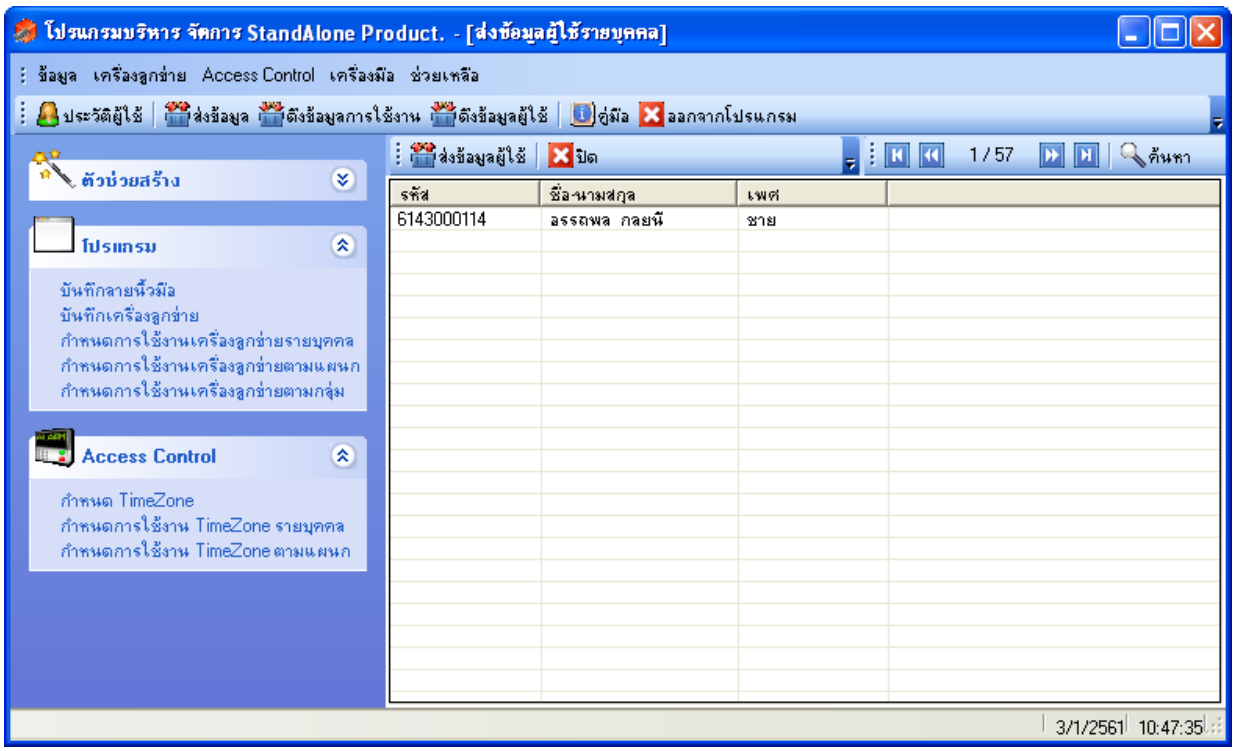
ภาพที่ 4.13 หน้าจอเกี่ยวกับการค้นหาข้อมูลผู้ใช้

ให้ใส่ชื่อ “อรรถพล”

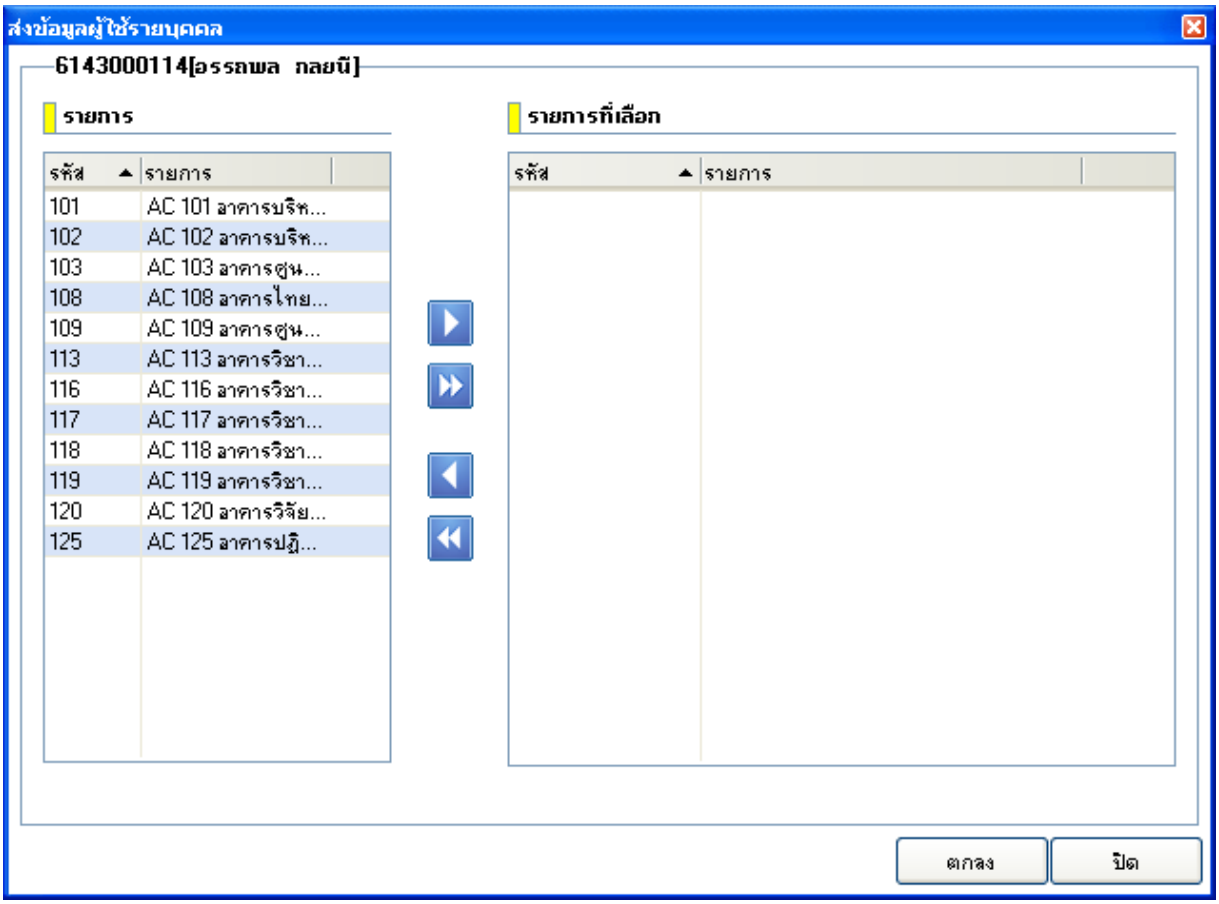


ภาพที่ 4.14 หน้าจอเกี่ยวกับการค้นหาข้อมูลผู้ใช้ของ “อรรถพล”

กดปุ่ม ตกลง

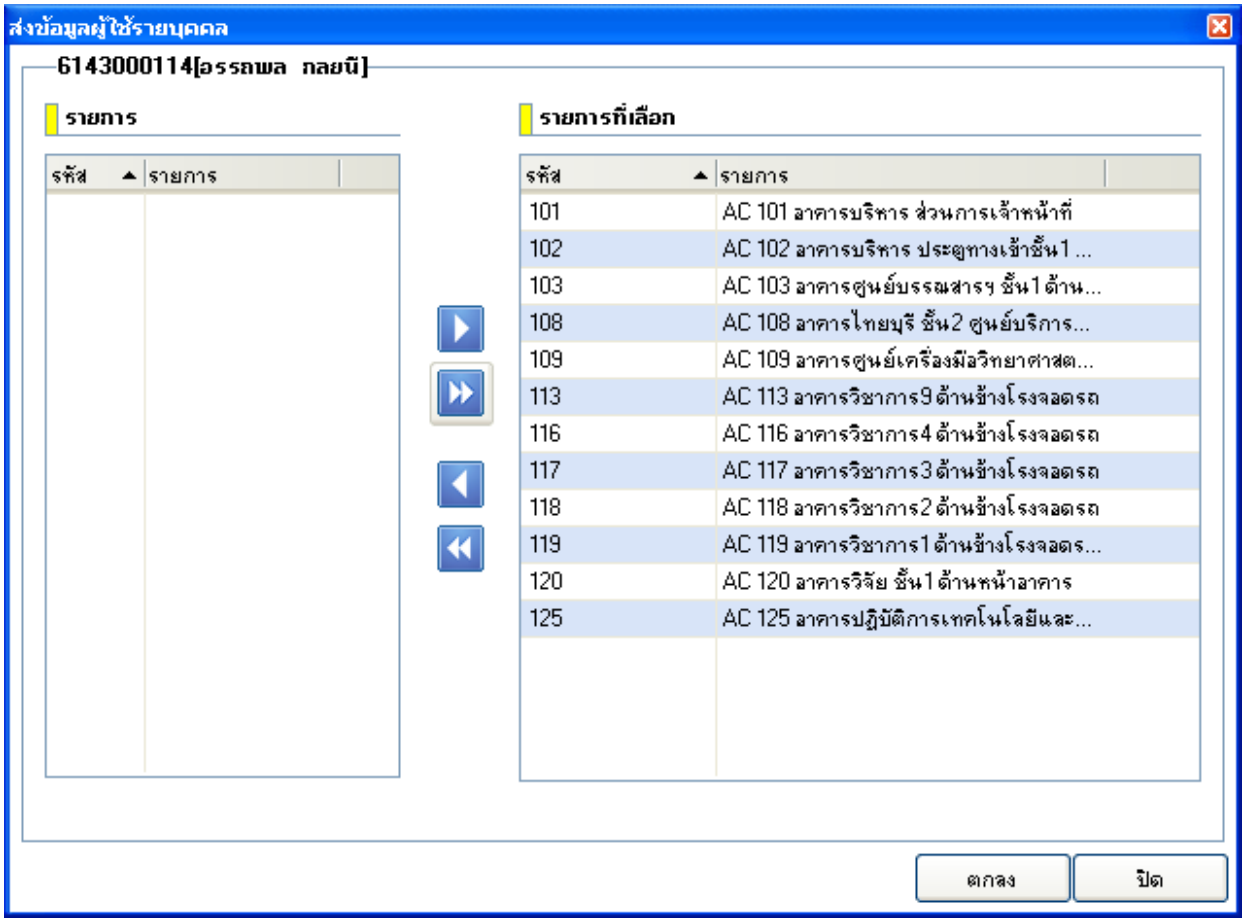


ภาพที่ 4.15 หน้าจอเกี่ยวกับการค้นหาพบข้อมูลผู้ใช้ของ “อรรถพล”



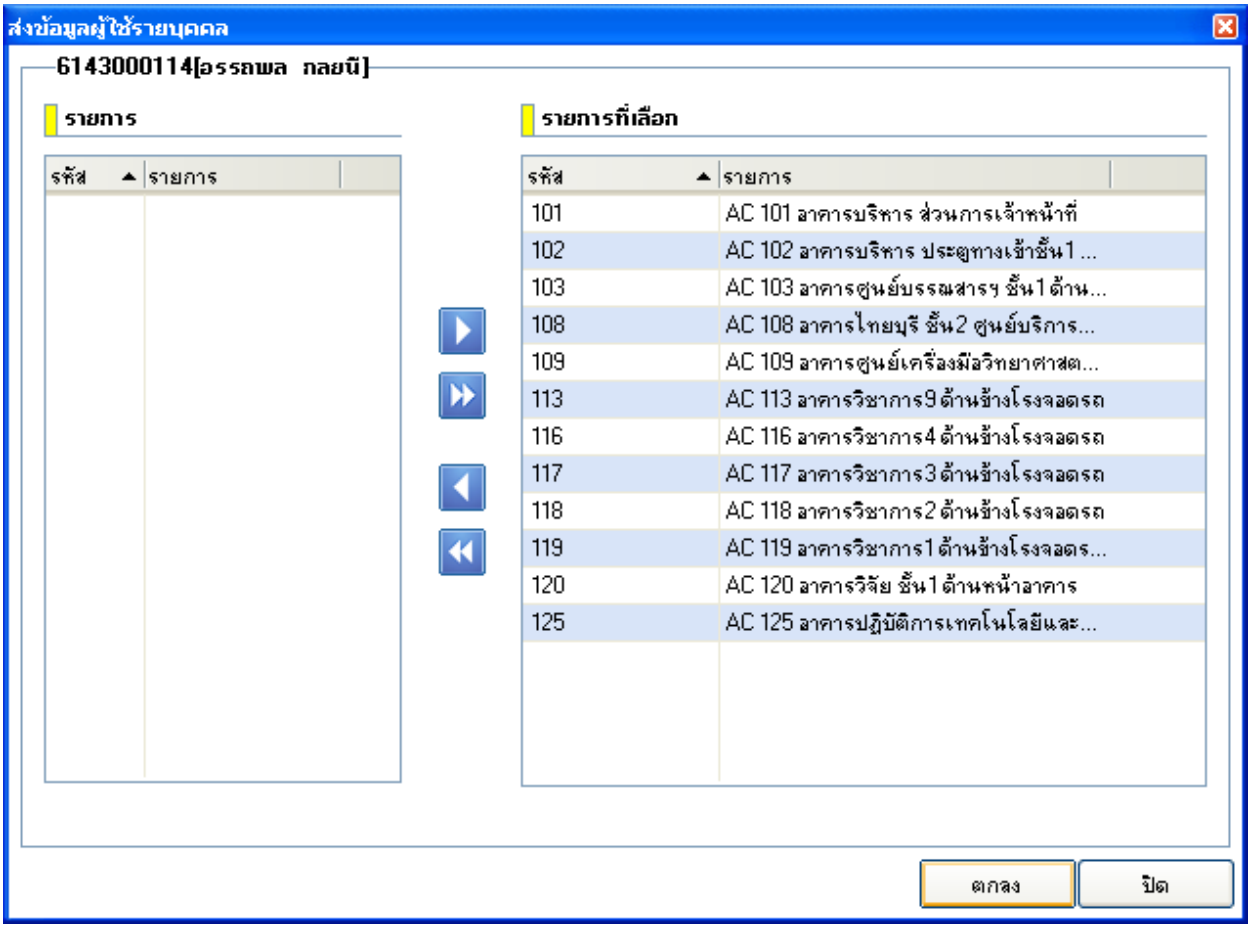
ภาพที่ 4.16 หน้าจอเกี่ยวกับการส่งข้อมูลผู้ใช้ของ “อรรถพล”

กดปุ่ม  ระบบของโปรแกรมจะนำข้อมูลรายการผู้ใช้ไปยังจุดรายการที่เลือก



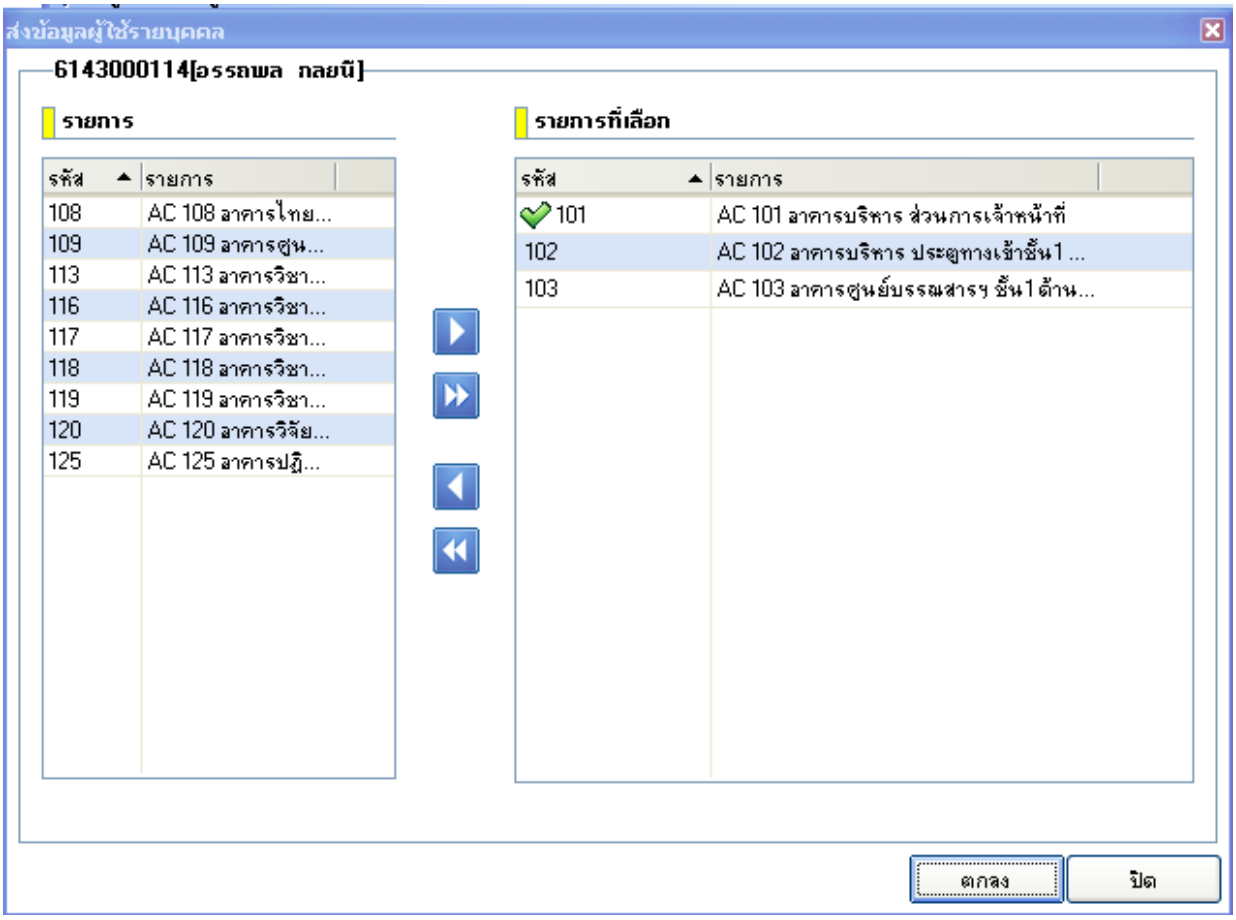
ภาพที่ 4.17 หน้าจอเกี่ยวกับการส่งข้อมูลผู้ใช้ของ “อรรถพล” ไปยังรายการที่เลือกไว้

กดปุ่ม ตกลง ระบบจะเริ่มส่งข้อมูลผู้ใช้ไปยังจุดที่กำหนดการใช้งาน



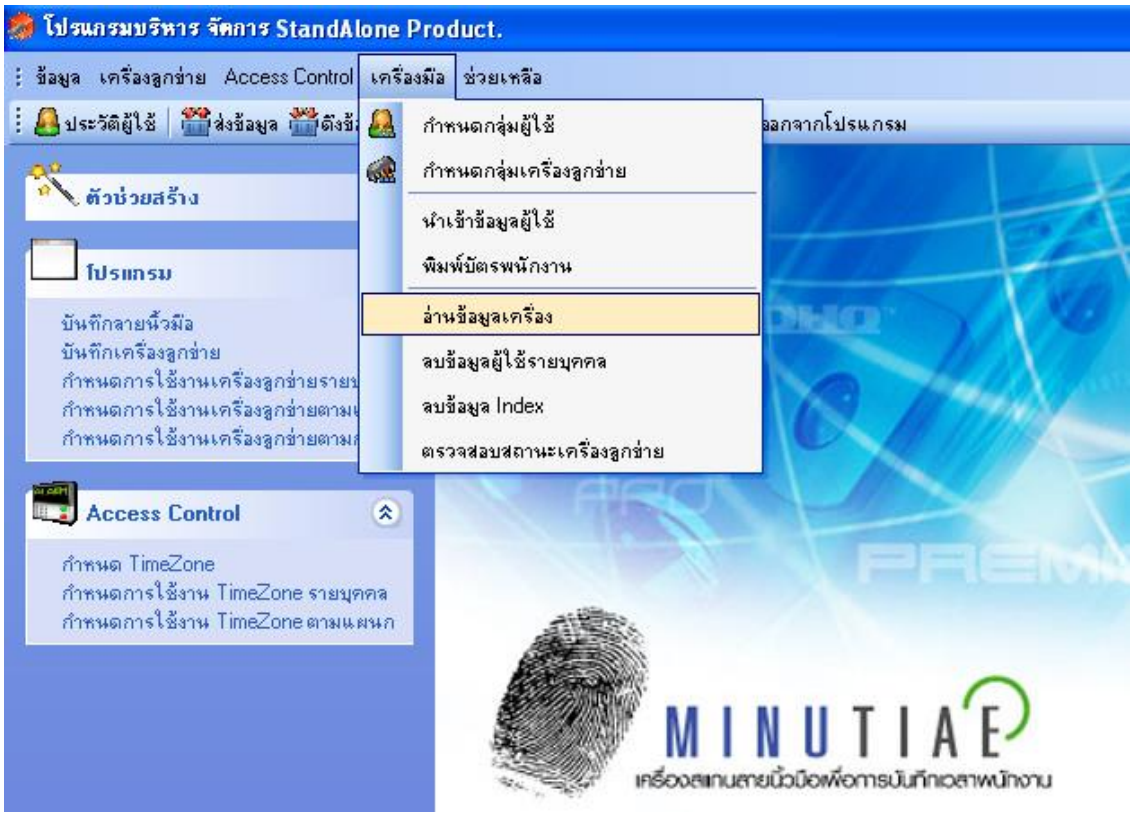
ภาพที่ 4.18 หน้าจอเกี่ยวกับการกดปุ่มตกลงเพื่อดำเนินการส่งข้อมูล

เมื่อระบบได้ทำการส่งข้อมูลสิทธิ์ รายการที่เลือกสำเร็จ จะปรากฏเครื่องหมายถูกสีเขียวดังภาพ



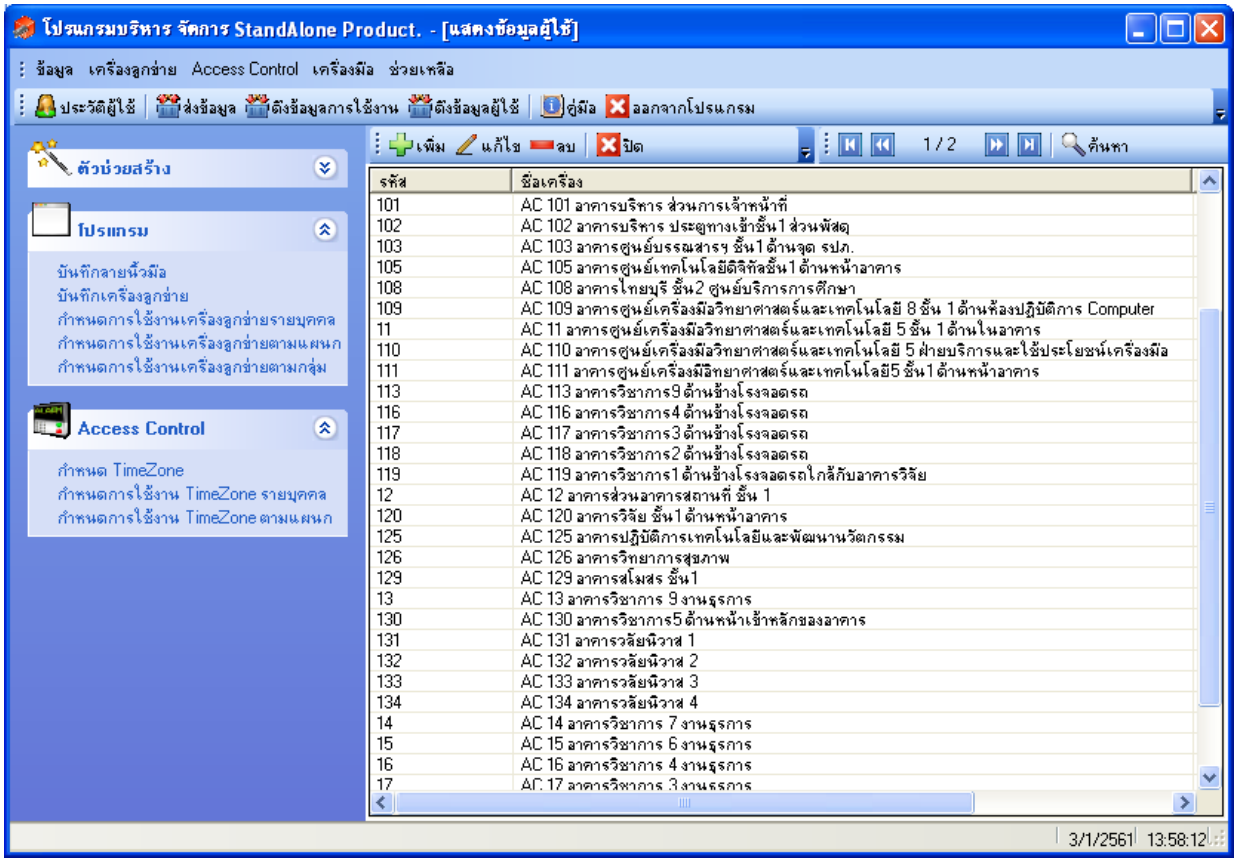
ภาพที่ 4.19 หน้าจอเกี่ยวกับระบบกำลังดำเนินการส่งข้อมูล

หากจะตรวจสอบว่าข้อมูลผู้ใช้ดังกล่าวไปยังจุดตามรายการที่เลือก ให้ไปที่เมนูเครื่องมือ เลือก “อ่านข้อมูลเครื่อง”



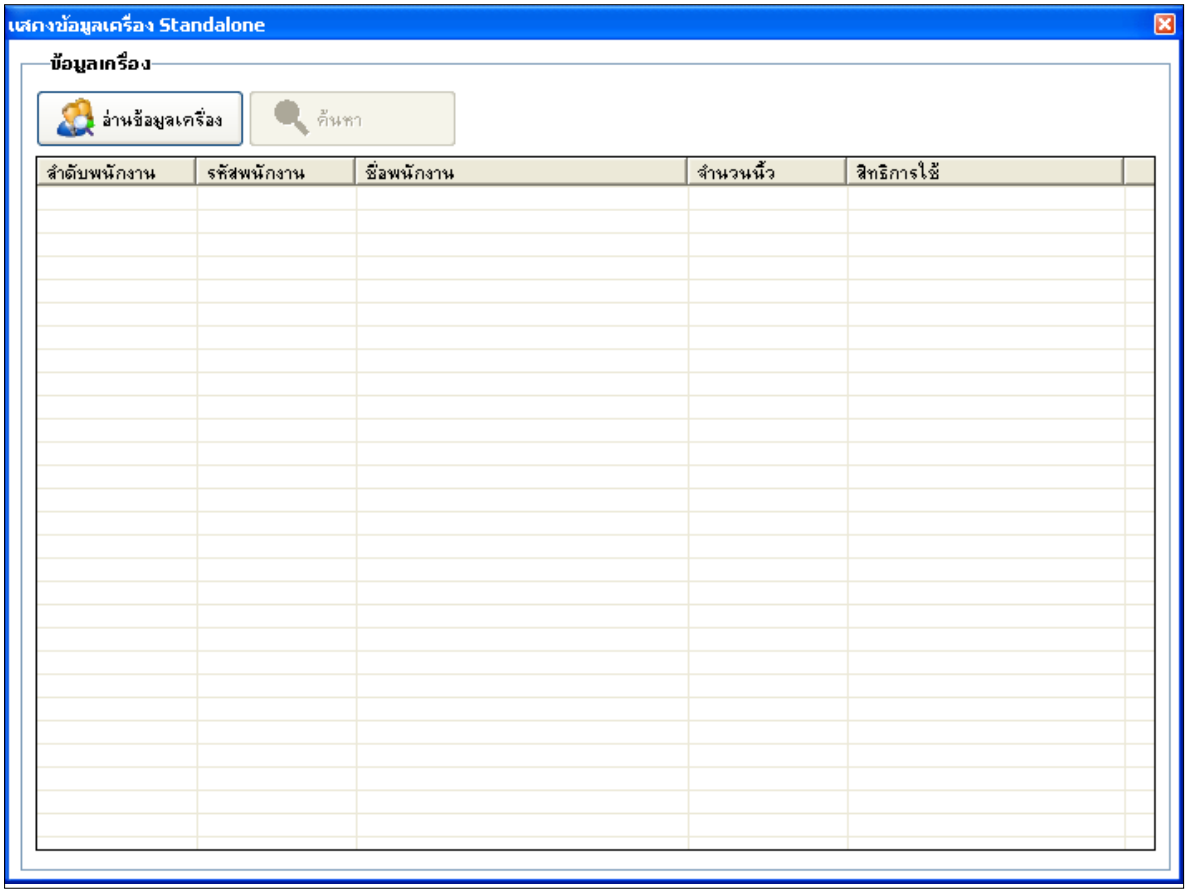
ภาพที่ 4.20 หน้าจอเกี่ยวกับการอ่านข้อมูลเครื่อง

จะได้หน้าจอ



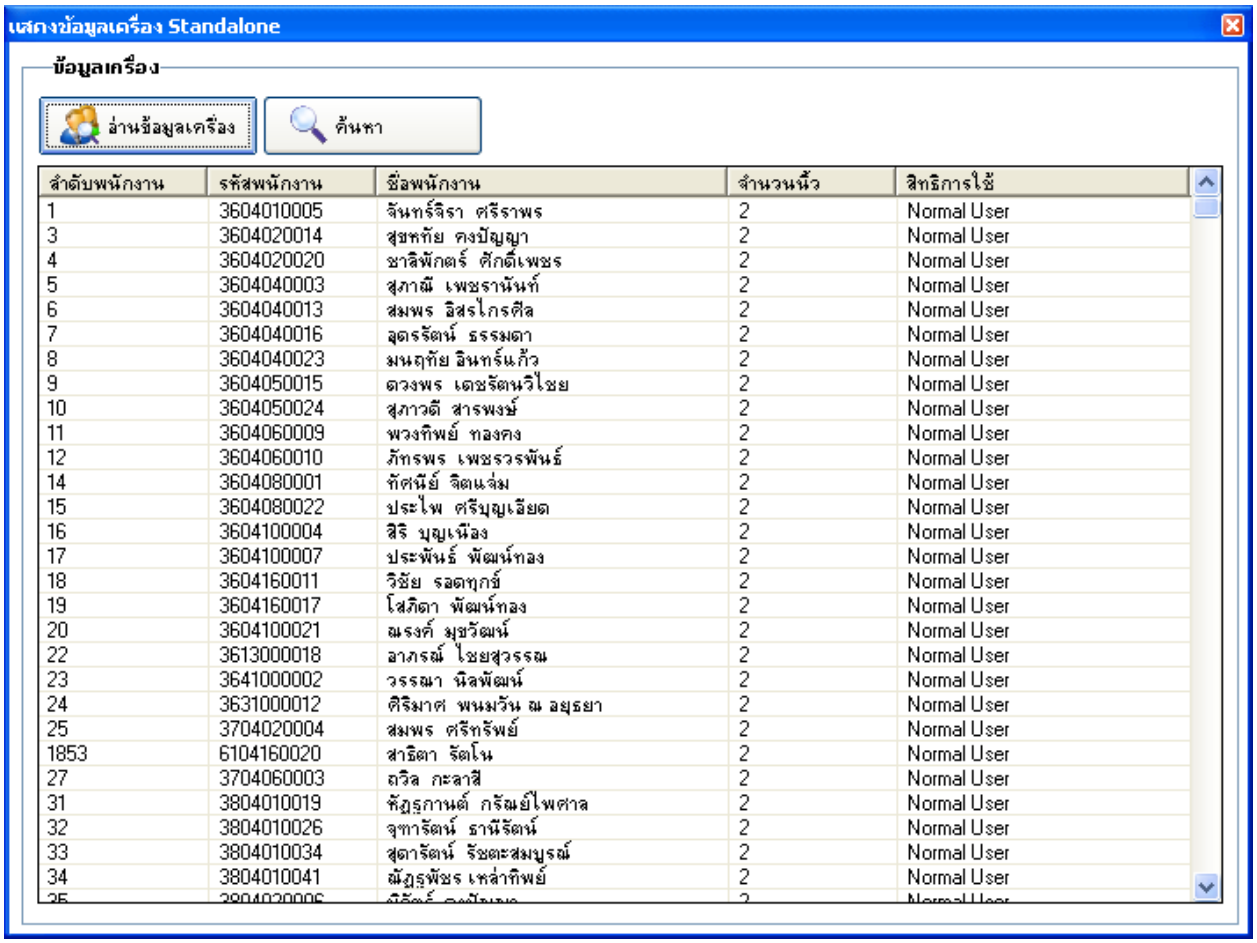
ภาพที่ 4.21 หน้าจอเกี่ยวกับรายละเอียดข้อมูลเครื่อง

สมมุติว่าในครั้งนี้อยากรู้ว่า ข้อมูลของ “อรรถพล” ปรากฏในจุดอาคารบริหาร ประตูทางเข้าชั้น 1 ส่วนพัสดุ หรือไม่ ให้กดเลือกชื่อเครื่อง AC102 แล้ว กดปุ่มอ่านข้อมูลเครื่อง

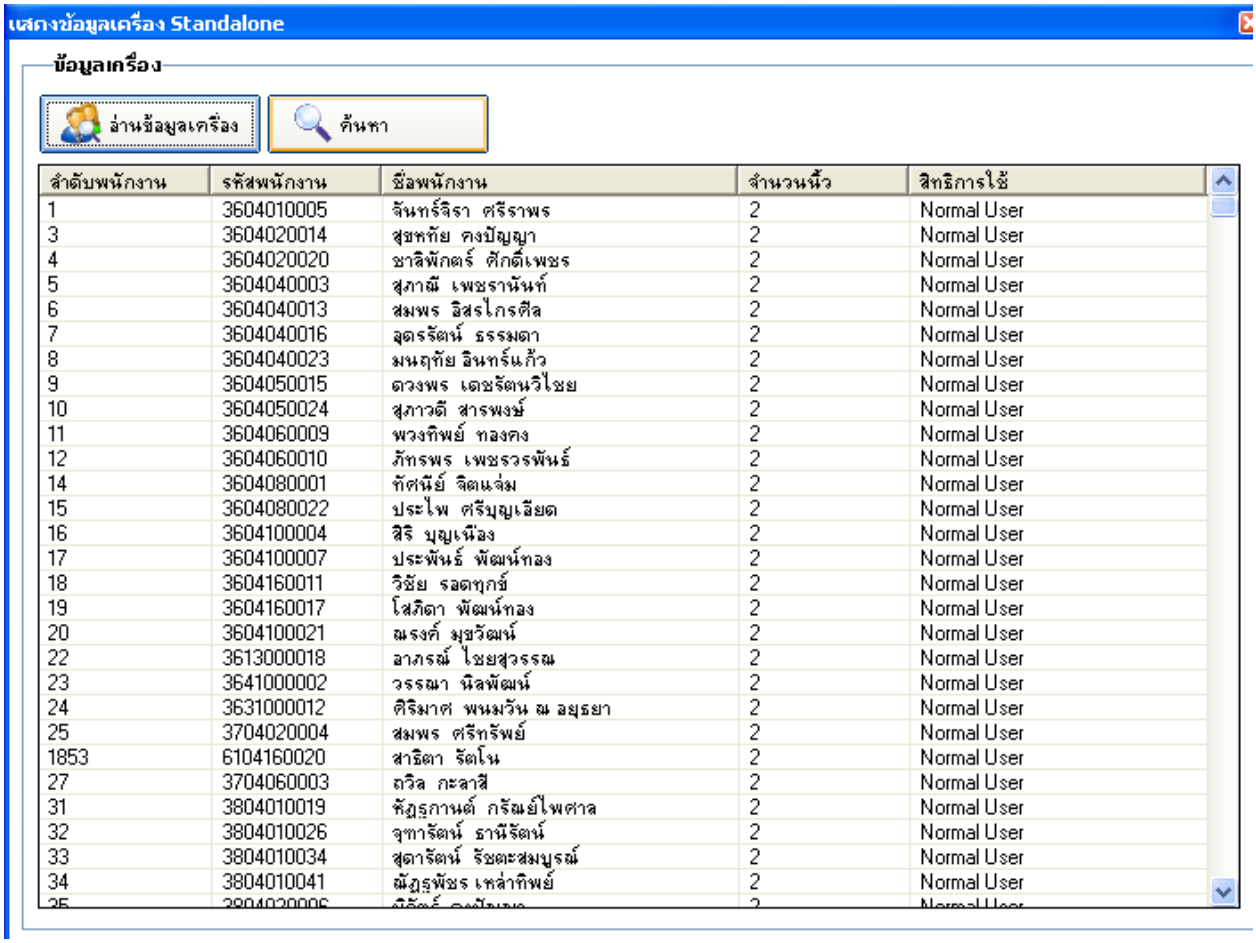


ภาพที่ 4.22 หน้าจอเกี่ยวกับการอ่านข้อมูลเครื่อง

จากนั้นเมื่อได้หน้าจอข้างล่างนี้ ให้ลองกดปุ่ม ค้นหา ชื่อ “อรรถพล” พนักงานที่ส่งสิทธิ์มาแล้ว ซึ่งจะเห็นชื่อผู้ใช้งานที่ทำการค้นหาปรากฏขึ้น

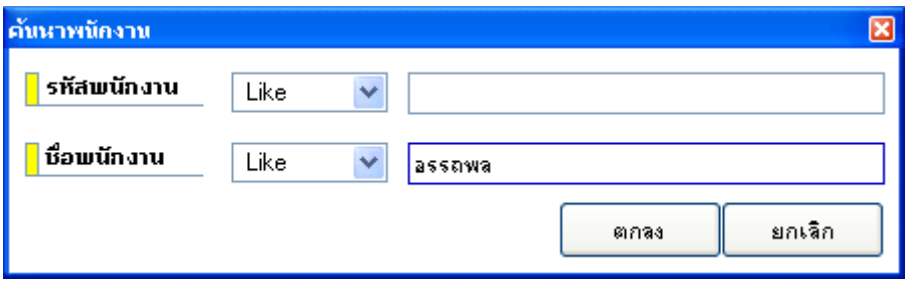


ภาพที่ 4.23 หน้าจอเกี่ยวกับผลการอ่านข้อมูลเครื่องสำเร็จ



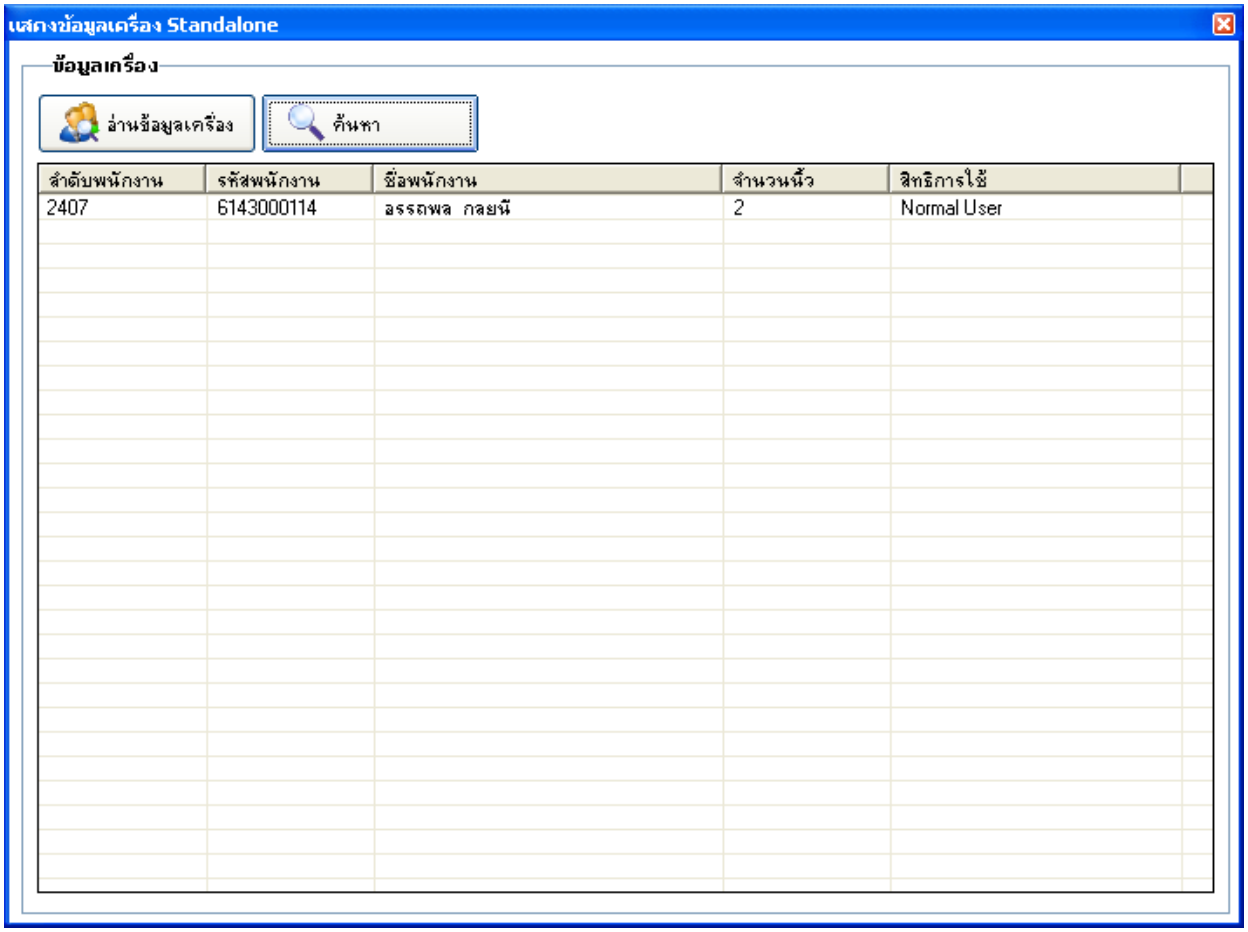
ภาพที่ 4.24 หน้าจอเกี่ยวกับผลการอ่านข้อมูลเครื่องสำเร็จและให้ค้นหา

ใส่ชื่อ “อรรถพล” ผู้ใช้งานที่ต้องการค้นหา กดปุ่ม ตกลง



ภาพที่ 4.25 หน้าจอเกี่ยวกับการค้นหา

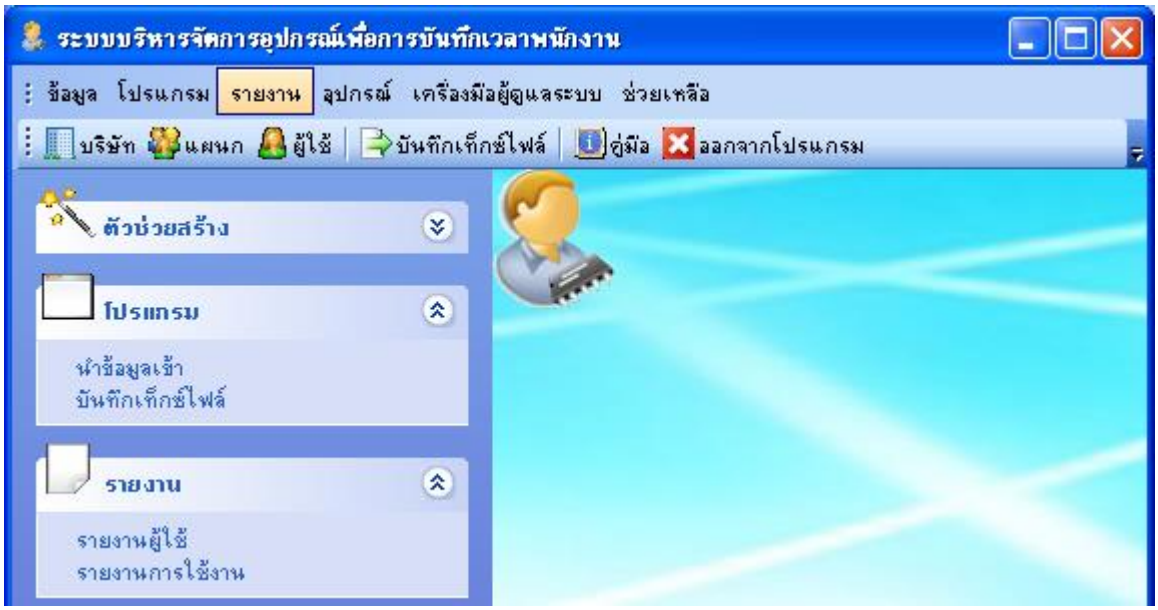
หากมีข้อมูลที่ค้นหาพบเจอจะปรากฏหน้าจอถัดมา



ภาพที่ 4.26 หน้าจอเกี่ยวกับแสดงผลของการค้นหา

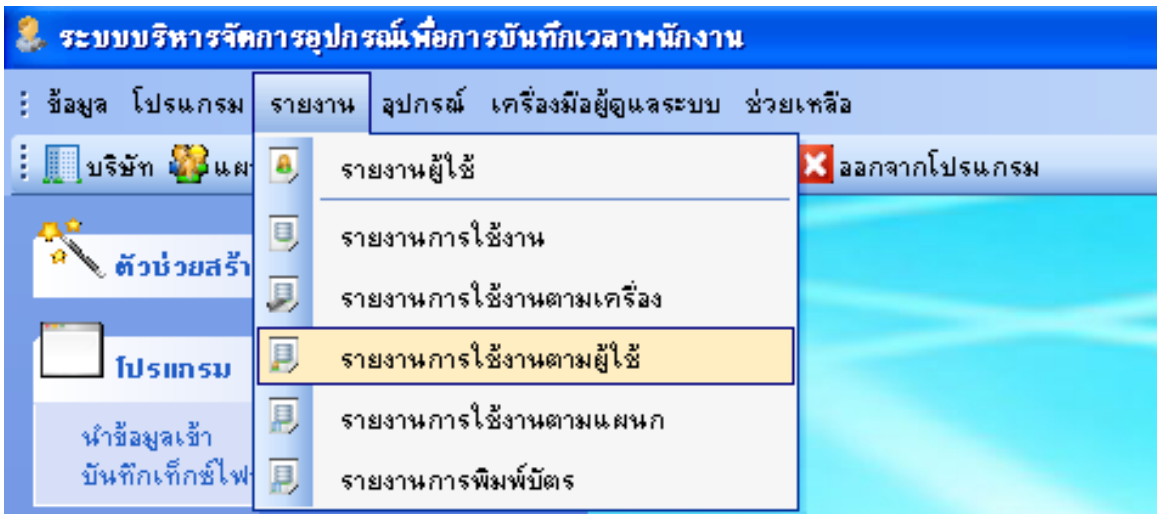
จะเห็นข้อมูลลายนิ้วมือ 2 นิ้ว และสิทธิ์การใช้เป็นแบบ Normal User คือผู้ใช้ทั่วไป ซึ่งสามารถสรุปผลได้ว่าการส่งสิทธิ์การใช้งานของพนักงานประสบความสำเร็จมีข้อมูลจำนวน 2 นิ้ว

5) ผลการทดสอบการใช้งาน เพื่อความถูกต้องให้ดูผลการใช้งานจากโปรแกรมที่เมนูรายงาน



ภาพที่ 4.27 หน้าจอเกี่ยวกับแสดงเมนูรายงาน

โดยเลือก “รายงานการใช้งานตามผู้ใช้”



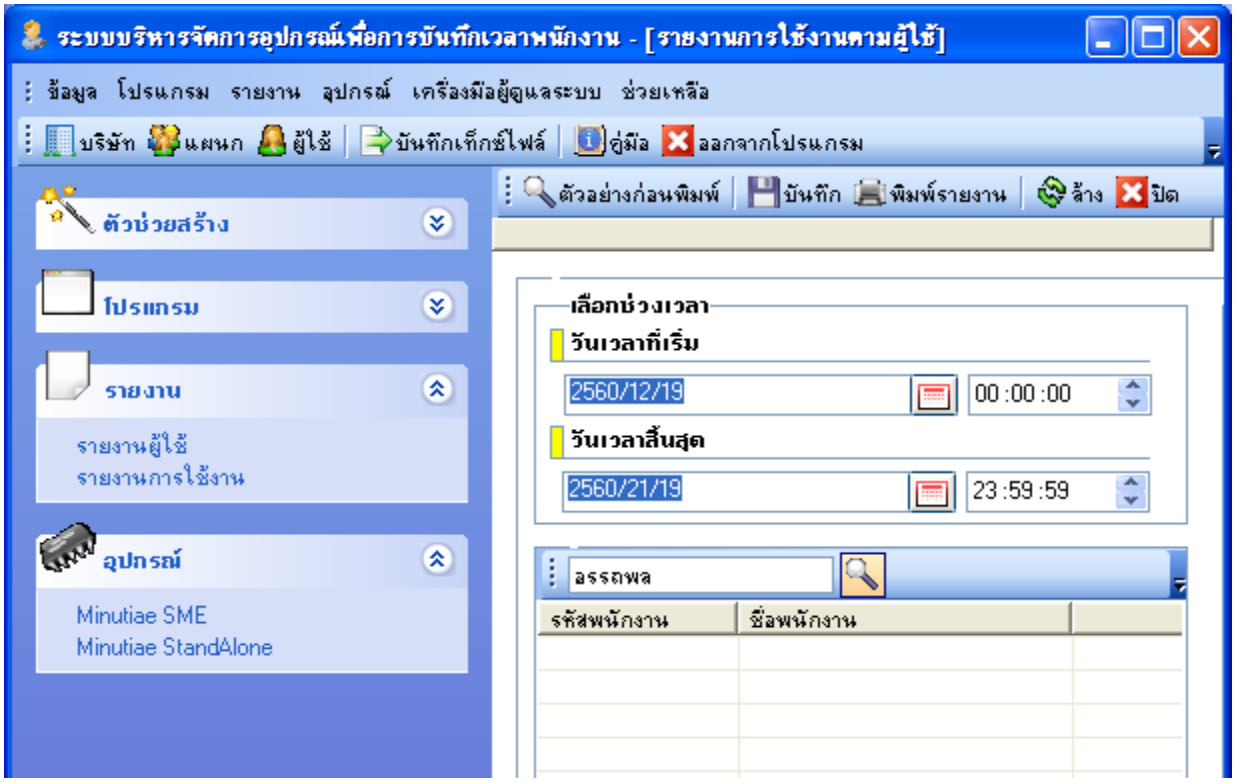
ภาพที่ 4.28 หน้าจอเกี่ยวกับแสดงเมนูรายงานการใช้งานตามผู้ใช้

ให้ทำการใส่ข้อมูล ดังนี้

1) ปี/เดือน/วันที่ และ เวลาเริ่มต้น

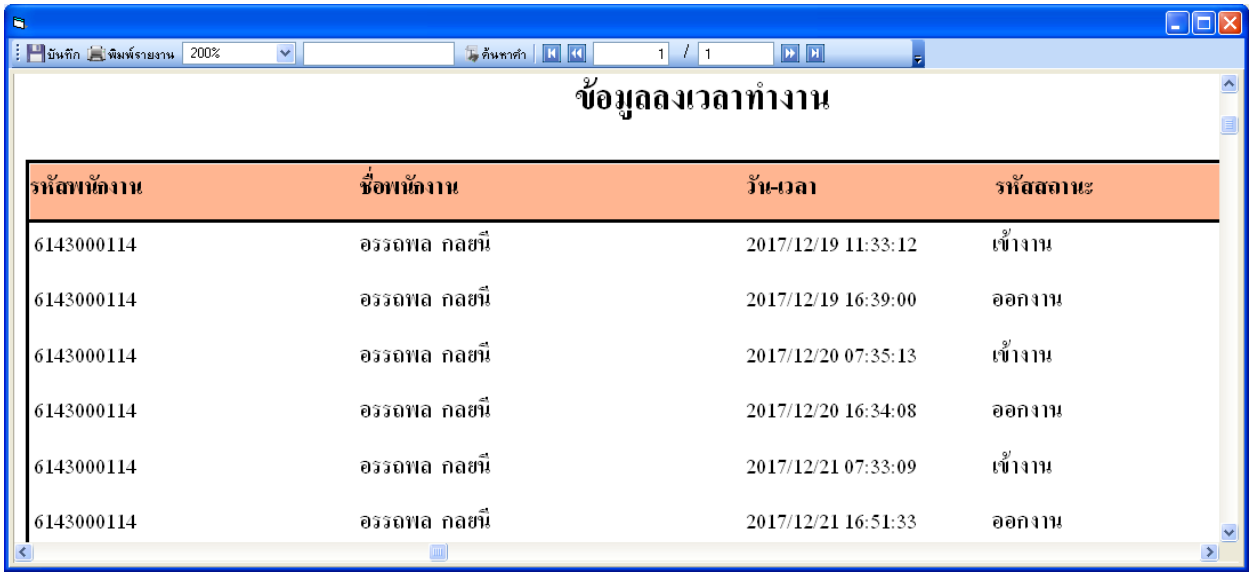
2) ปี/เดือน/วันที่ และ เวลาสิ้นสุด

3) ชื่อผู้ใช้ที่ต้องดูรายงาน

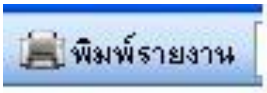


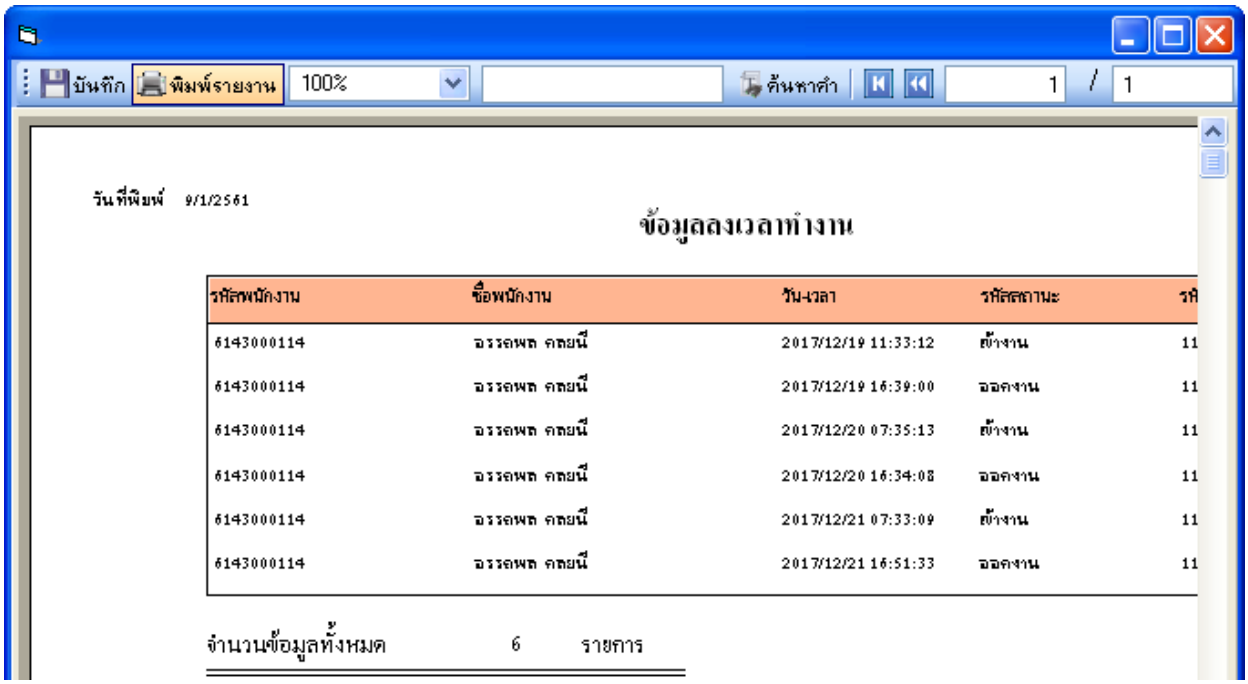
ภาพที่ 4.29 หน้าจอเกี่ยวกับการให้กรอกข้อมูลในเมนูรายงานการใช้งานตามผู้ใช้

เมื่อกดปุ่ม ตัวอย่างก่อนพิมพ์ รายงานการใช้งานตามผู้ใช้ จะได้รายงาน



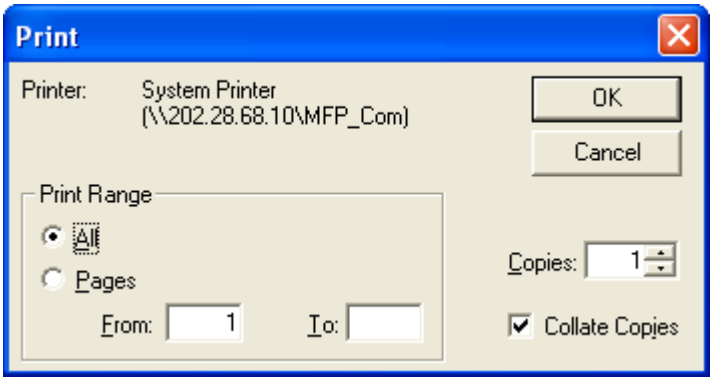
ภาพที่ 4.30 หน้าจอเกี่ยวกับแสดงรายงานการใช้งานตามผู้ใช้

หากต้องการสั่งพิมพ์ให้กดปุ่มพิมพ์รายงาน 



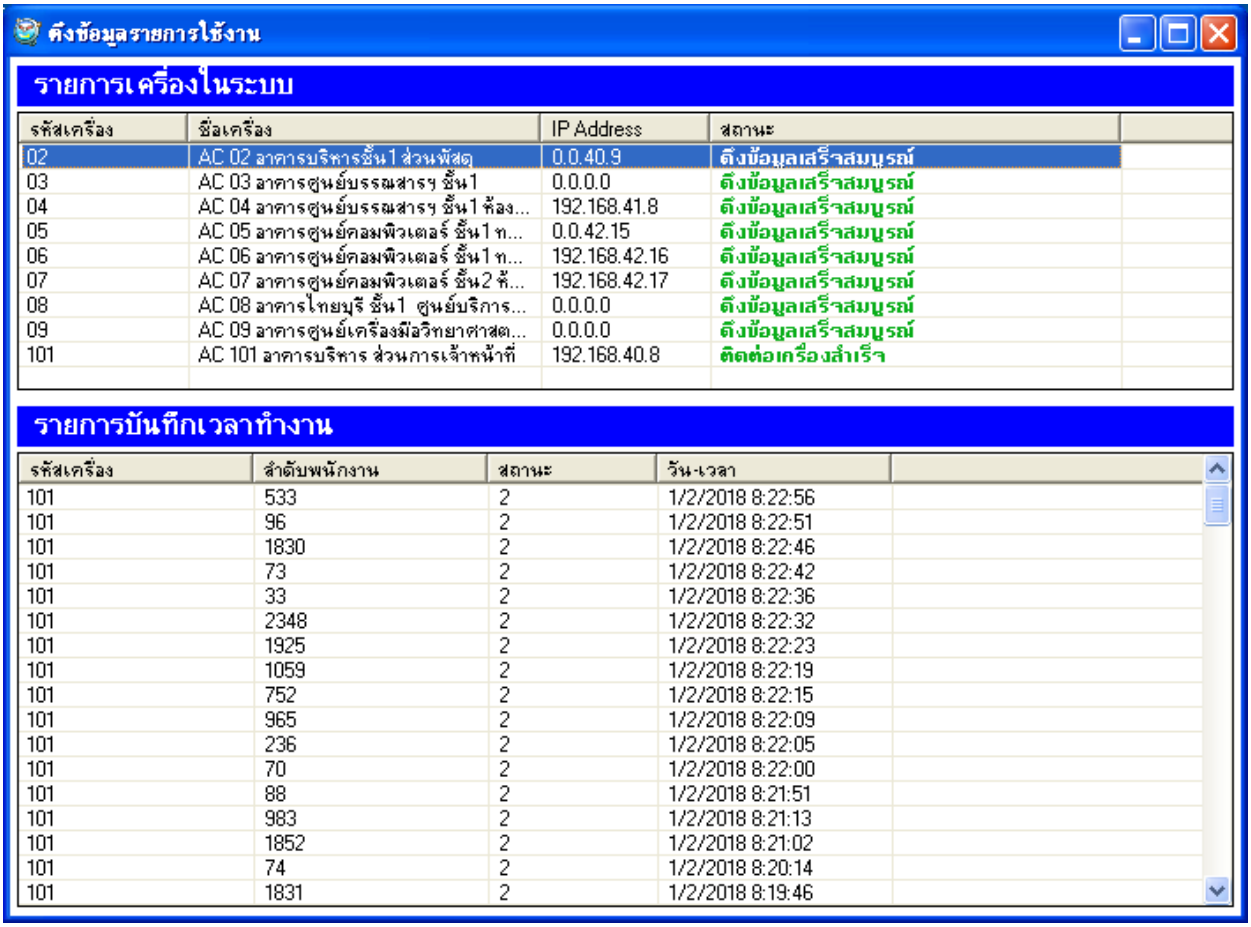
ภาพที่ 4.31 หน้าจอเกี่ยวกับแสดงเมนูการพิมพ์รายงานการใช้งานตามผู้ใช้

มีหน้าจอการสั่งพิมพ์ ให้ระบุจำนวนหน้าที่ต้องการ แล้ว กดปุ่ม OK นับเป็นการสั่งพิมพ์ที่สำเร็จ

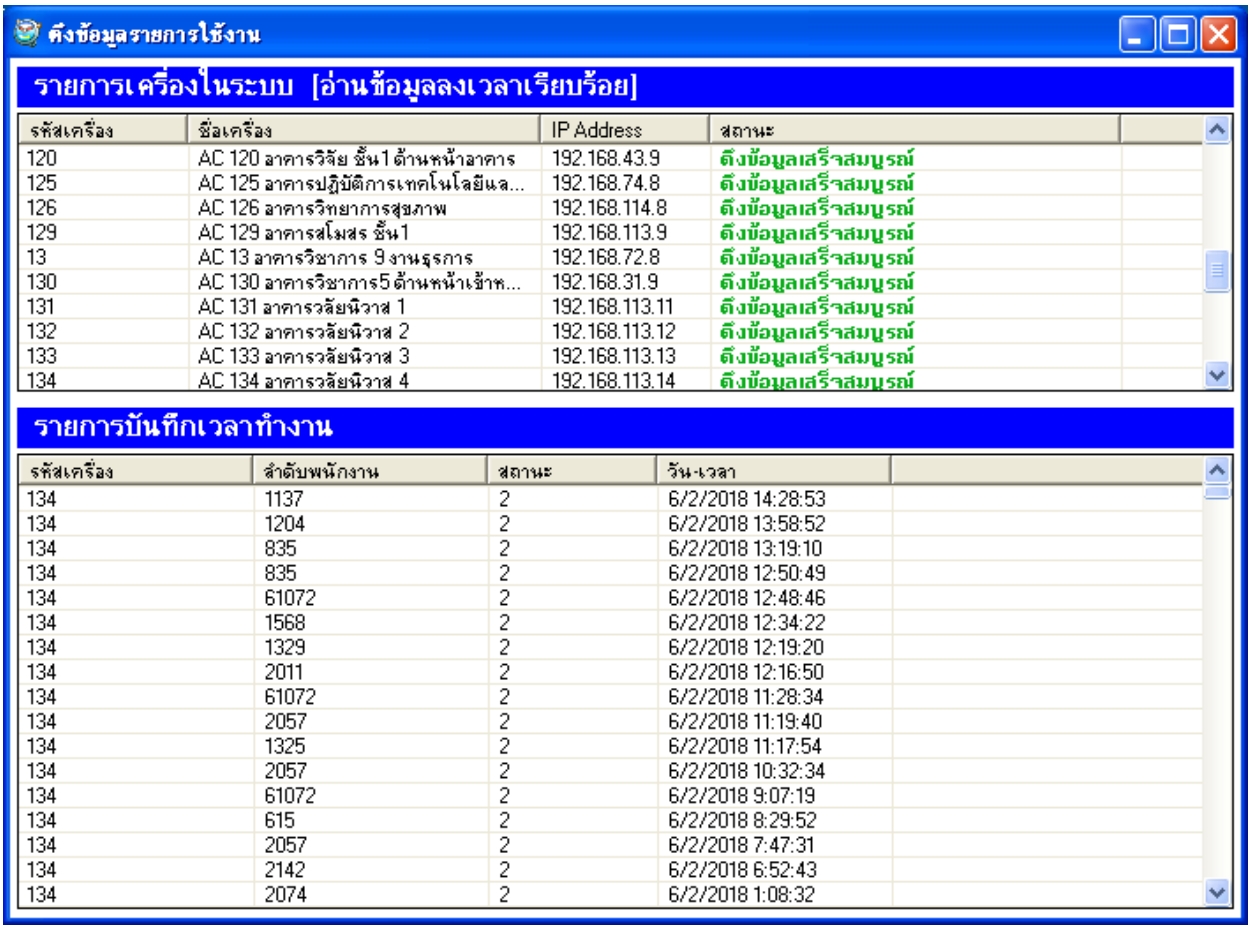


ภาพที่ 4.32 หน้าจอเกี่ยวกับแสดงเมนูการใส่ค่าจำนวนการสั่งพิมพ์รายงานการใช้งานตามผู้ใช้

6) นำเข้าข้อมูลการลงเวลาปฏิบัติงาน เป็นการกำหนดให้โปรแกรม DownloadTrans.exe ทำงานในเวลาที่ตั้งไว้เพื่อทำการดึงข้อมูลการลงเวลา เข้าสู่ฐานข้อมูลกลางเป็นรอบรายละ 1 ชั่วโมงของทุกวัน

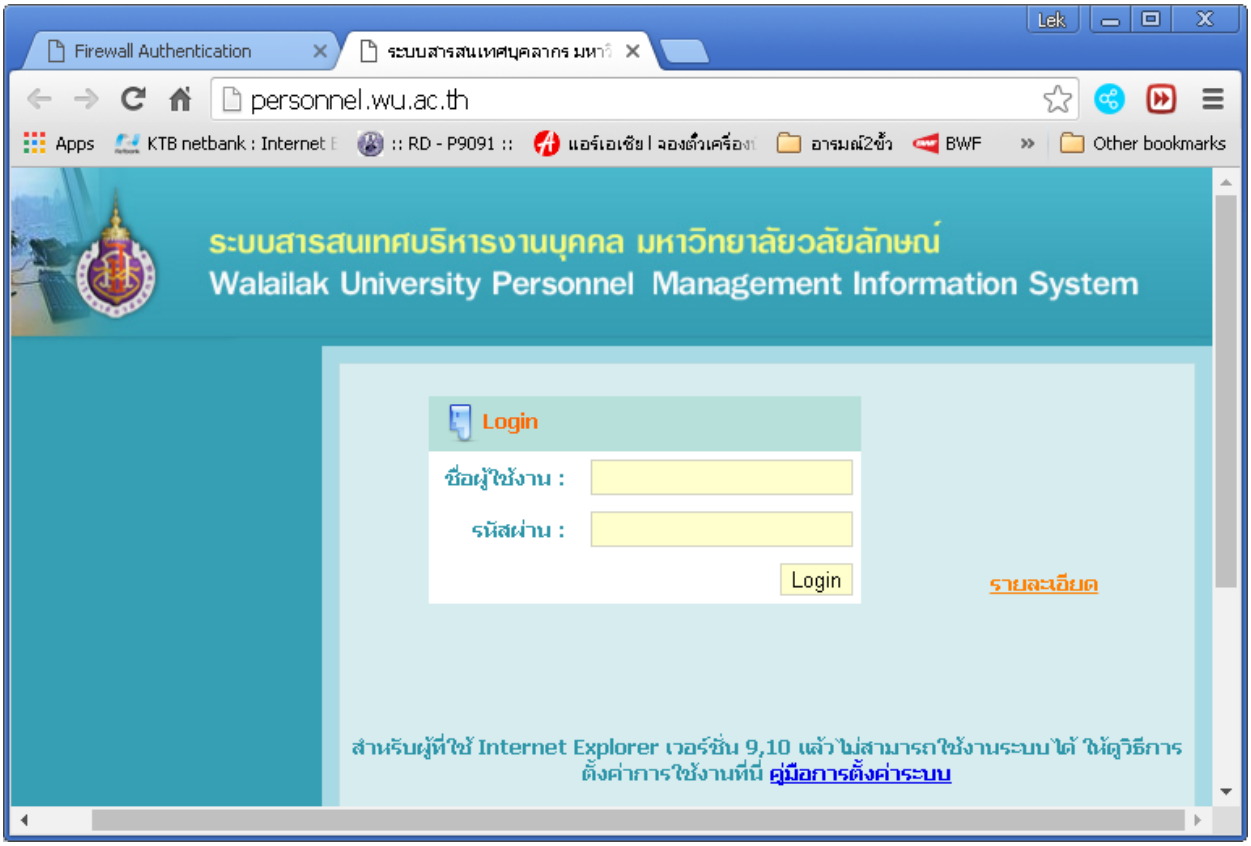


ภาพที่ 4.33 หน้าจอเกี่ยวกับแสดงการดึงข้อมูลการลงเวลา



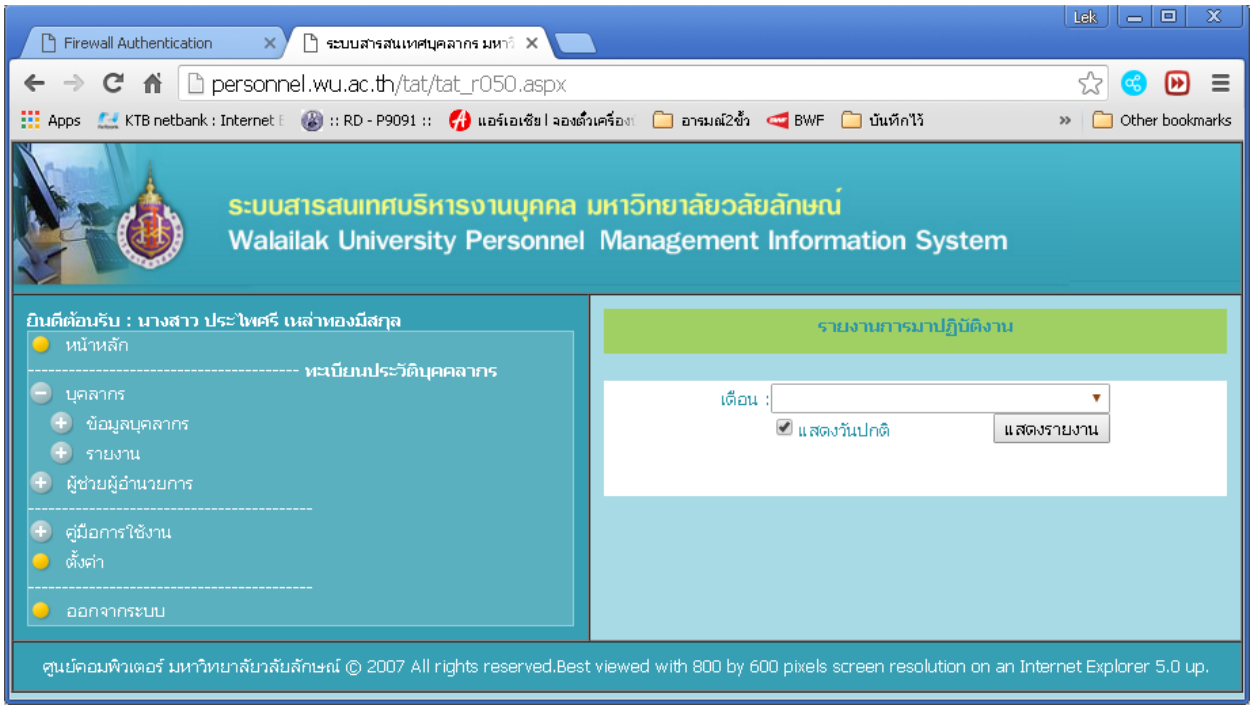
ภาพที่ 4.34 หน้าจอเกี่ยวกับแสดงการดึงข้อมูลการลงเวลาที่สำเร็จ

7) รายงานการลงเวลาปฏิบัติงาน สามารถดูรายงานได้จากการเข้าเว็บ http://personnel.wu.ac.th/



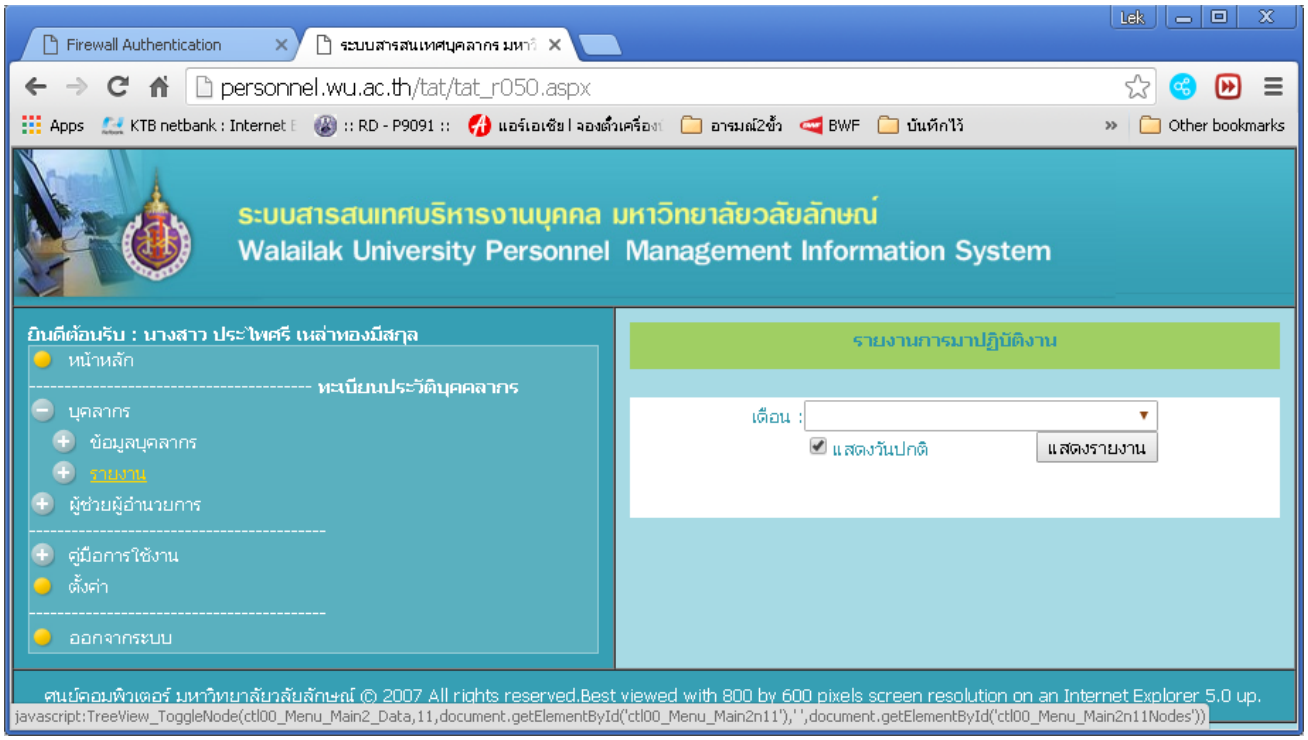
ภาพที่ 4.35 หน้าจอเกี่ยวกับเว็บระบบสารสนเทศบริหารงานบุคคล

โดยใส่ชื่อผู้ใช้งาน และ รหัสผ่าน และกดปุ่ม Login จะได้หน้าจอเกี่ยวกับเว็บระบบสารสนเทศบริหารงานบุคคลที่ Login เพื่อดูรายงาน

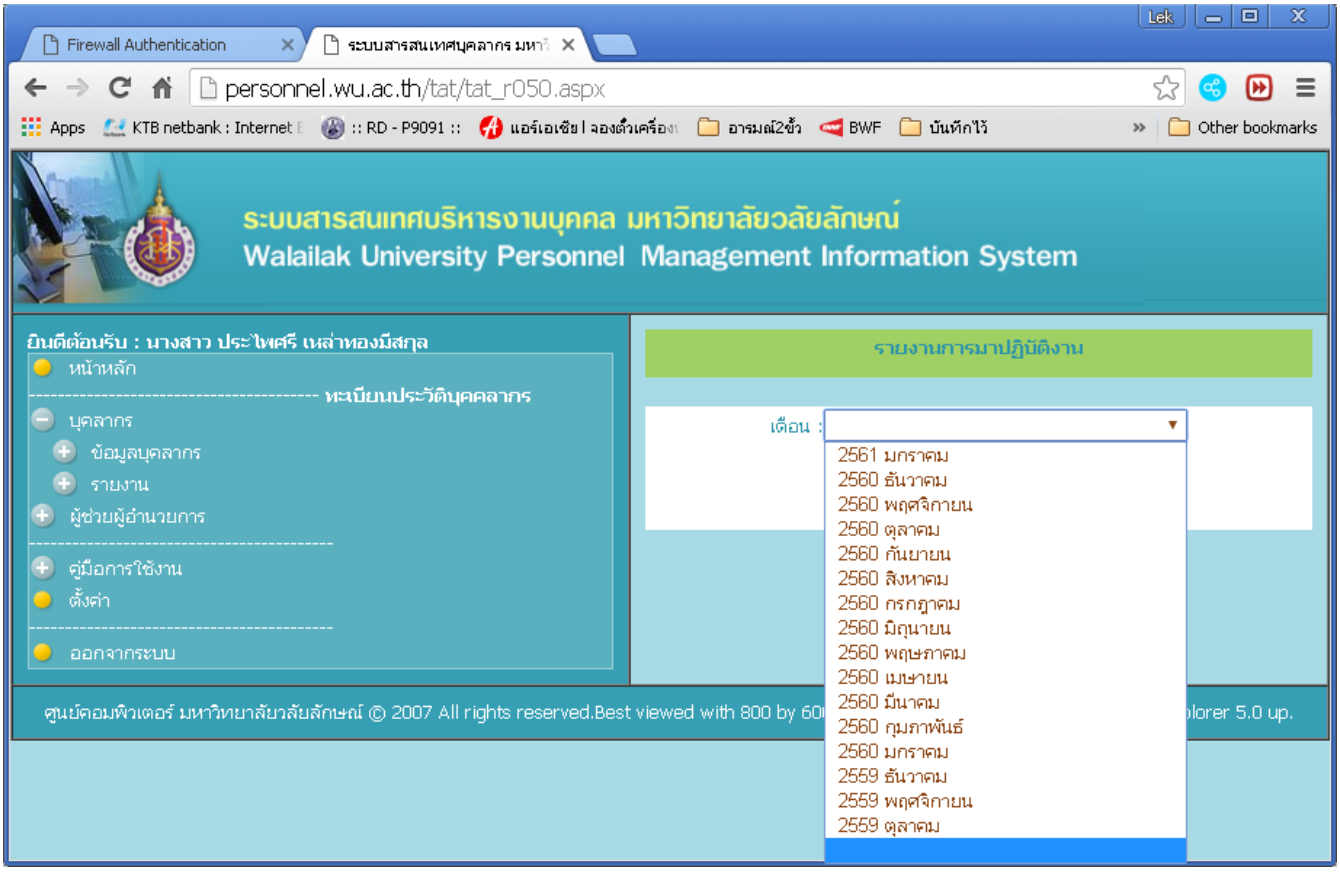


ภาพที่ 4.36 หน้าจอเกี่ยวกับเว็บระบบสารสนเทศบริหารงานบุคคลที่ Login เพื่อดูรายงาน

เลื่อนเมาส์ Click ที่เมนู “รายงาน”

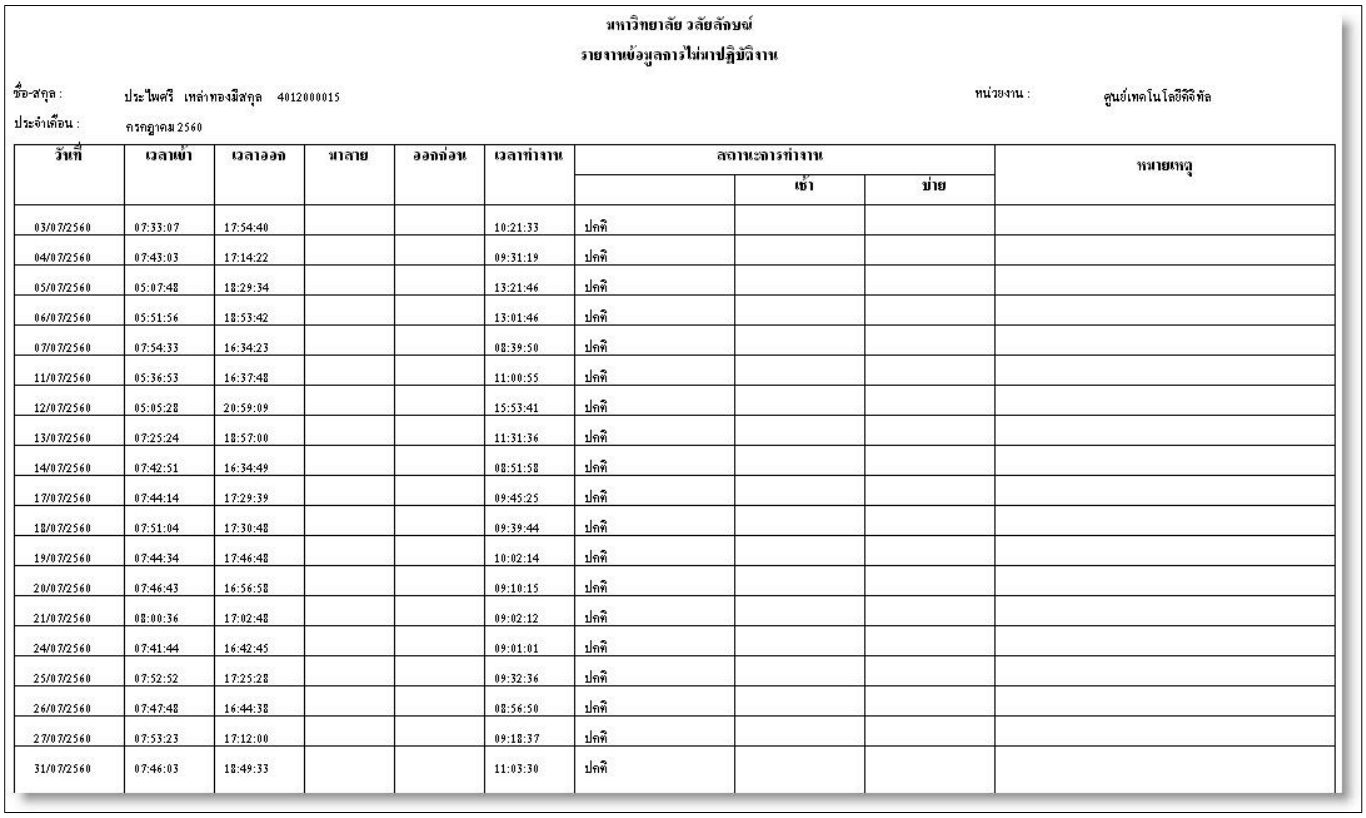


ภาพที่ 4.37 หน้าจอเกี่ยวกับการดูรายงานแบบเลือกเดือนที่ต้องการ



ภาพที่ 4.38 หน้าจอเกี่ยวกับการดูรายงานแบบเลือกเดือนที่ต้องการ เช่น 2560 กรกฎาคม

เลื่อนเมาส์เพื่อเลือกดูเดือนที่ต้องการดูรายงานการมาปฏิบัติงานแล้ว จะปรากฏรายงานที่ต้องการ



มหาวิทยาลัย วลัยลักษณ์

รายงานข้อมูลการไม่มาปฏิบัติงาน

ชื่อ-สกุล : ประไพศรี เหล่าทองมีสกุล 4012000015 หน่วยงาน : ศูนย์เทคโนโลยีดิจิทัล

ประจำเดือน : กรกฎาคม 2560

วันที่	เวลาเข้า	เวลาออก	มาสาย	ออกก่อน	เวลาทำงาน	สถานะการทำงาน			หมายเหตุ
							เช้า	บ่าย	
03/07/2560	07:33:07	17:54:40			10:21:33	ปกติ			
04/07/2560	07:43:03	17:14:22			09:31:19	ปกติ			
05/07/2560	05:07:48	18:29:34			13:21:46	ปกติ			
06/07/2560	05:51:56	18:53:42			13:01:46	ปกติ			
07/07/2560	07:54:33	16:34:23			08:39:50	ปกติ			
11/07/2560	05:36:53	16:37:48			11:00:55	ปกติ			
12/07/2560	05:05:28	20:59:09			15:53:41	ปกติ			
13/07/2560	07:25:24	18:57:00			11:31:36	ปกติ			
14/07/2560	07:42:51	16:34:49			08:51:58	ปกติ			
17/07/2560	07:44:14	17:29:39			09:45:25	ปกติ			
18/07/2560	07:51:04	17:30:48			09:39:44	ปกติ			
19/07/2560	07:44:34	17:46:48			10:02:14	ปกติ			
20/07/2560	07:46:43	16:56:58			09:10:15	ปกติ			
21/07/2560	08:00:36	17:02:48			09:02:12	ปกติ			
24/07/2560	07:41:44	16:42:45			09:01:01	ปกติ			
25/07/2560	07:52:52	17:25:28			09:32:36	ปกติ			
26/07/2560	07:47:48	16:44:38			08:56:50	ปกติ			
27/07/2560	07:53:23	17:12:00			09:18:37	ปกติ			
31/07/2560	07:46:03	18:49:33			11:03:30	ปกติ			

ภาพที่ 4.39 หน้าจอเกี่ยวกับรายงานแบบเลือกเดือนที่ต้องการ เช่น 2560 กรกฎาคม

4.4 เทคนิคการติดตามและประเมินผลการปฏิบัติงาน

เมื่อดำเนินการตามคู่มือการปฏิบัติงานเล่มนี้ มีวิธีเพื่อติดตามให้ทราบผลการทำงานได้โดย

1) การตรวจดูรายงานการใช้งานตามผู้ใช้ ที่เพิ่งกำหนดการใช้งานให้ไปนั้น สามารถใช้งานได้แล้วจริง ซึ่งในรายงานจะระบุให้ทราบถึงผู้ใช้ เริ่มใช้งานได้ตั้งแต่วัน-เวลา สถานะการเข้างาน-ออกงาน

รหัสพนักงาน	ชื่อพนักงาน	วัน-เวลา	รหัสสถานะ
6143000114	อรรถพล คชยนี	2017/12/19 11:33:12	เข้างาน
6143000114	อรรถพล คชยนี	2017/12/19 16:39:00	ออกงาน
6143000114	อรรถพล คชยนี	2017/12/20 07:35:13	เข้างาน
6143000114	อรรถพล คชยนี	2017/12/20 16:34:08	ออกงาน
6143000114	อรรถพล คชยนี	2017/12/21 07:33:09	เข้างาน
6143000114	อรรถพล คชยนี	2017/12/21 16:51:33	ออกงาน

จำนวนข้อมูลทั้งหมด 6 รายการ

ภาพที่ 4.40 หน้าจอเกี่ยวกับรายงานการใช้งานตามผู้ใช้

2) สามารถโทรไปสอบถามพนักงานใหม่ผู้นั้นที่เบอร์โต๊ะทำงาน หลังจากที่ส่งสิทธิ์ผู้ใช้ไปเรียบร้อยแล้ว ทั้งนี้ หากทราบว่า พนักงานใหม่ ผู้ใช้งานไม่สามารถวางนิ้วเพื่อสแกนลายนิ้วมือได้ ต้องไปดูที่หน้างาน ณ ตำแหน่งที่ใช้งานจริงเพื่อให้เห็นว่า ลายนิ้วมือของพนักงานมีสภาพเปลี่ยนแปลงไปจากเดิมที่เคยเก็บไว้หรือไม่ ซึ่งหากเปลี่ยนแปลงจากเดิมต้องทำการเก็บลายนิ้วมือใหม่อีกครั้ง

3) กรณีงานล่าช้าในขั้นตอนข้อมูลพนักงานใหม่ที่แจ้งมาไม่ถูกต้อง ปรับแก้ไขใช้เวลานานกว่า 1 วัน ให้พนักงานใหม่แจ้งในระบบ e-Services ศูนย์เทคโนโลยีดิจิทัล เพื่อประเมินความพึงพอใจในการรับบริการ มีระดับความพึงพอใจ 1 ถึง 5 รวม 3 ด้าน ได้แก่ (1) สามารถดำเนินงานได้เรียบร้อย (2) การดำเนินงานเป็นไปตามกำหนดเวลาที่เหมาะสม และ (3) Service Mind ของผู้ให้บริการ และสามารถเพิ่มข้อเสนอแนะหรือความคิดเห็นเพื่อปรับปรุงการทำงานให้มีประสิทธิภาพยิ่งขึ้น

4.5 เทคนิคการทำให้ผู้รับบริการพึงพอใจ

ในการปฏิบัติงานเพื่อให้ผู้รับบริการเกิดความพึงพอใจ ผู้เขียนได้แบ่งผู้รับบริการออกเป็น 2 กลุ่ม ดังนี้

4.5.1 กลุ่มเจ้าหน้าที่บริหารงานทั่วไป ส่วนทรัพยากรมนุษย์และองค์กร

งานระบบสแกนลายนิ้วมือเป็นเครื่องมือสำคัญที่จะช่วยสร้างความพึงพอใจให้กับเจ้าหน้าที่บริหารงานทั่วไปที่รับผิดชอบงานด้านรายงานการมาปฏิบัติงานของระบบสารสนเทศบริหารงานบุคคล ซึ่งรายงานที่ออกมาในแต่ละเดือนของพนักงานและลูกจ้าง ต้องมีความถูกต้องแม่นยำที่เป็นรูปแบบมาตรฐานและมีความน่าเชื่อถือ เป็นรายงานที่สามารถแสดงเวลาของการเข้างาน รายงานที่สามารถแสดงเวลาของการออกงาน รายงานที่สามารถแสดงสถานะการเข้างาน รายงานที่สามารถแสดงสถานะการออกงาน รายงานที่สามารถแสดงตำแหน่งของอาคารที่ไปสแกนลายนิ้วมือ รายงานที่สามารถสืบค้นข้อมูลการสแกนลายนิ้วมือตามชื่อ-สกุล หรือรหัสพนักงาน (ภาพที่ 4.41)

ภาพที่ 4.41 รายงานแสดงรายเดือน

4.5.2 กลุ่มพนักงานและลูกจ้าง ที่เป็นพนักงานใหม่

งานระบบสแกนลายนิ้วมือเป็นเครื่องมือสำคัญที่จะช่วยสร้างความพึงพอใจให้กับพนักงานใหม่ด้วยรายงานที่สามารถแสดงข้อมูลการสแกนลายนิ้วมือทั้งการเข้า/ออกงานของวันที่มาปฏิบัติงาน

รายงานที่สามารถแสดงข้อมูลการสแกนลายนิ้วมือเป็นรายสัปดาห์ รายงานที่สามารถแสดงการสืบค้นข้อมูลการสแกนลายนิ้วมือเป็นรายวัน-สัปดาห์-เดือน-ปี (ภาพที่ 4.42)

ภาพที่ 4.42 รายงานแสดงข้อมูลการสแกนลายนิ้วมือ

การปฏิบัติงานเพื่อให้ผู้รับบริการทั้ง 2 กลุ่ม ได้รับการบริการที่พึงพอใจ งานระบบสแกนลายนิ้วมือมีระบบประเมินผลการรับบริการที่พนักงานเปิดแจ้งใบงานในระบบ e-Services ศูนย์เทคโนโลยีดิจิทัล ซึ่งทุกใบงานได้ส่งถึงผู้บังคับบัญชาของหน่วยงานหลังจากนั้นจะแจ้งให้ทราบเป็นรายเดือนเพื่อก่อให้เกิดการพัฒนางานที่ดำเนินงานให้มีประสิทธิภาพและประสิทธิผล

4.6 จรรยาบรรณ/คุณธรรม/จริยธรรมในการปฏิบัติงาน

ในการปฏิบัติงานตามคู่มือระบบสแกนลายนิ้วมือเพื่อลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ ผู้ปฏิบัติงานควรยึดหลักปฏิบัติจริยธรรม คุณธรรม และจรรยาบรรณ ตามข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยประมวลจริยธรรมและธรรมาภิบาลนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัยวลัยลักษณ์ พ.ศ. 2565 ลักษณะที่ 2 ประมวลจริยธรรมและหลักธรรมาภิบาล ส่วนที่ 4 จริยธรรมและจรรยาบรรณของบุคลากร ซึ่งประกอบด้วย

1) ยืนหยัดกระทำในสิ่งที่ถูกต้องและเป็นธรรม

2) มีจิตสำนึกที่ดี รับผิดชอบต่อหน้าที่ เสียสละ ปฏิบัติหน้าที่ด้วยความรวดเร็ว โปร่งใสตรวจสอบได้และคุ้มค่า

3) แยกเรื่องส่วนตัวออกจากตำแหน่งหน้าที่ และยึดถือประโยชน์ส่วนรวมมากกว่าประโยชน์ส่วนตัวและประโยชน์ส่วนบุคคล

4) ไม่ใช้ตำแหน่งหน้าที่แสวงหาผลประโยชน์โดยมิชอบ และไม่กระทำการอันเป็นการขัดกันระหว่างผลประโยชน์ส่วนตนและประโยชน์ส่วนรวม รวมทั้งกระทำในลักษณะผลประโยชน์ทับซ้อน

5) เคารพและปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และมติสภามหาวิทยาลัยอย่างครบถ้วนตรงไปตรงมา

6) ปฏิบัติหน้าที่ด้วยความซื่อสัตย์สุจริต เป็นกลางทางการเมือง ให้บริการแก่ประชาชนโดยมีอัธยาศัยที่ดี และมีความเป็นธรรม

7) มุ่งผลสัมฤทธิ์ของงาน รักษาคุณภาพและมาตรฐานแห่งวิชาชีพโดยเคร่งครัด

8) เป็นแบบอย่างที่ดีในการดำรงตน รักษาชื่อเสียงและภาพลักษณ์ของมหาวิทยาลัยโดยรวม

9) ต้องไม่ปฏิบัติงานข้ามขั้นตามลำดับชั้นการบังคับบัญชาโดยไม่ได้รับอนุญาต ไม่ปิดบังซ่อนเร้นข้อราชการอันอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัย รวมทั้งไม่ละเมิดหรือละเว้นการปฏิบัติหน้าที่โดยมิชอบ

10) ไม่ยินยอมให้ผู้อื่นใช้หน้าที่หรืออำนาจของตนแสวงหาผลประโยชน์อันมิชอบ

11) ละเว้นการให้สัมภาษณ์ การอภิปราย การปาฐกถา การบรรยาย หรือการวิพากษ์วิจารณ์ในลักษณะเลือกข้าง อันอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัย ราชการ หรือความเป็นกลางทางการเมือง เว้นแต่เป็นการแสดงความคิดเห็นตามหลักวิชาการอันสุจริต

12) ไม่คัดลอก หรือขโมยผลงานของผู้อื่นมาเป็นของตนโดยเจตนา

13) ต้องส่งเสริม รักษาชื่อเสียงและภาพลักษณ์ของมหาวิทยาลัย

บทที่ 5
ปัญหา อุปสรรค แนวทางแก้ไข การพัฒนาและข้อเสนอแนะ

จากการวิเคราะห์สภาพแวดล้อมภายในและภายนอกด้วยวิธี SWOT Analysis ในการให้บริการระบบสแกนลายนิ้วมือเพื่อลงเวลาปฏิบัติงาน ที่ผ่านมาพบจุดแข็ง จุดอ่อน โอกาส และอุปสรรค สรุปได้ว่า

จุดแข็ง (Strengths)	จุดอ่อน (Weaknesses)
1) มีโปรแกรมบริหารจัดการเวอร์ชัน 3.0 เพื่อเชื่อมต่อกับอุปกรณ์สแกนลายนิ้วมือที่มีความเสถียรภาพ	1) ข้อมูลลายนิ้วมือของพนักงานและลูกจ้าง ที่สัมผัสกับคราบน้ำมัน สารเคมี แอลกอฮอล์ ความเย็น มีผลให้ลายนิ้วมือบางเปลี่ยนสภาพไป
2) มีฐานข้อมูลเป็น Oracle เพื่อเชื่อมต่อในระบบฐานข้อมูลหลักของมหาวิทยาลัย	2) ข้อมูลลายนิ้วมือของพนักงานและลูกจ้าง ที่ทานยาบางประเภท มีผลให้ลายนิ้วมือบางและเปลี่ยนสภาพ
3) มีระบบสารสนเทศบริหารงานบุคคล เพื่อออกรายงานของพนักงานและลูกจ้างเป็นรายวัน รายเดือน รายปี	3) ข้อมูลลายนิ้วมือของพนักงานและลูกจ้าง ที่ได้รับการรักษาด้วยยาเคมีบำบัด มีผลให้ลายนิ้วมือบางและเปลี่ยนสภาพ
4) ข้อมูลลายนิ้วมือของพนักงานและลูกจ้างถูกเก็บรักษาในฐานข้อมูลกลางใช้เฉพาะภายในมหาวิทยาลัย	4) เครื่องสแกนลายนิ้วมือ รุ่น Standalone รองรับการใช้งานได้เพียง 800 คน และอายุการใช้งานมากกว่า 10 ปี
5) เครื่องสแกนลายนิ้วมือติดตั้งภายในและนอกเขตการศึกษา รวม 35 จุด เพื่อรองรับการใช้งานให้คลอบคลุมทั่วถึง	5) เลนส์ของเครื่องสแกนลายนิ้วมือ รุ่น Standalone มีอายุการใช้งานเพียง 1 ปี
6) เครื่องสแกนลายนิ้วมือ MATHER รุ่น M-800 รองรับการใช้งานของพนักงานและลูกจ้างได้มากกว่า 8,000 คน และมีอายุการใช้งานอยู่ที่ 1 - 5 ปี	6) แหล่งจ่ายไฟสำรองของเครื่องสแกนลายนิ้วมือ รุ่น Standalone สำรองไฟให้ใช้งานได้เพียง 5 นาที (กรณีไฟฟ้าดับ)

โอกาส (Opportunities)	อุปสรรค (Threats)
1) ปรับเปลี่ยนเครื่องสแกนลายนิ้วมือ รุ่น Standalone แทนด้วยเครื่องสแกนลายนิ้วมือ MATHER รุ่น M-800 รวม 14 เครื่อง	1) ไม่ได้รับแจ้งผ่านเมลถึงจำนวนการจัดเก็บลายนิ้วมือพนักงานใหม่ จากส่วนทรัพยากรมนุษย์และองค์กร
2) หาแนวทางสำหรับการลงเวลาปฏิบัติงานเป็นรูปแบบใหม่ที่ใช้งบประมาณให้น้อยกว่าการปรับเปลี่ยนเครื่อง	2) ส่วนทรัพยากรมนุษย์และองค์กร นำเข้าข้อมูลไม่ถูกต้อง
3) ทดลองใช้ Application Timestamp Camera บนสมาร์ตโฟนเพื่อการเช็คอินเวลาและภาพถ่ายแทนการสแกนลายนิ้วมือ	3) พนักงานและลูกจ้างแจ้งว่าไม่สามารถสแกนลายนิ้วมือเพื่อลงเวลาเข้า-ออกงาน
	4) ข้อมูลการสแกนลายนิ้วมือ นำเข้าฐานข้อมูลกลางไม่ครบสมบูรณ์
	5) ข้อมูลรายงานแสดงการสแกนลายนิ้วมือทั้งการเข้า-ออกงานของวันที่มาปฏิบัติงานไม่ถูกต้อง เนื่องจากการลืมสแกนลายนิ้วมือ

จากผลการวิเคราะห์สภาพแวดล้อมภายในและภายนอกด้วยวิธี SWOT Analysis ดังกล่าวข้างต้นทำให้ทราบปัญหา อุปสรรค แนวทางแก้ไข การพัฒนาและข้อเสนอแนะ

5.1 ปัญหาอุปสรรคในการปฏิบัติงานและแนวทางแก้ไข

เมื่อผู้ปฏิบัติงานได้ใช้คู่มือเล่มนี้ จากประสบการณ์การทำงานมากกว่า 10 ปี ผู้เขียนพอสรุปปัญหาและแนวทางแก้ไขได้พอสังเขปในตารางที่ 5.1

ตารางที่ 5.1 ปัญหา/อุปสรรค แนวทางแก้ไข

ขั้นตอน	ปัญหา/อุปสรรค	แนวทางแก้ไข
1) นำเข้าข้อมูลพนักงานใหม่	เมื่อส่วนทรัพยากรมนุษย์และองค์กรนำเข้าข้อมูลพนักงานใหม่แล้ว แต่ลืมส่ง e-mail มาแจ้งให้งานระบบ finger Scan	ขอให้ส่วนทรัพยากรมนุษย์และองค์กร ดำเนินการส่ง e-mail มาแจ้งให้งานระบบ finger Scan ทันที
2) ตรวจสอบพร้อมปรับแก้ข้อมูลให้ถูกต้อง	เมื่อส่วนทรัพยากรมนุษย์และองค์กร ส่ง e-mail มาแจ้งให้งานระบบ finger Scanแล้วมีข้อมูลชื่อ-สกุลไม่ถูกต้อง	งานระบบ finger Scan ตรวจสอบพร้อมปรับแก้ไขชื่อ-สกุลให้ถูกต้อง
3) กำหนดสิทธิ์ให้กับพนักงานใหม่	งานระบบ finger Scan กำหนดสิทธิ์ให้ไม่ครบตามจุดใช้งาน	ดำเนินการกำหนดสิทธิ์เพิ่มให้ครบตามจุดใช้งาน
4) ส่งข้อมูลสิทธิ์ให้กับพนักงานใหม่	งานระบบ finger Scan ส่งสิทธิ์ให้ไม่ครบตามจุดใช้งาน	ดำเนินการกำหนดส่งสิทธิ์เพิ่มให้ครบตามจุดใช้งาน
5) ผลการทดสอบการใช้งาน	พนักงานไม่สามารถสแกนลายนิ้วมือเพื่อการเข้างาน/การออกงาน	1) ให้ดูข้อมูลสิทธิ์ของพนักงานว่ามีข้อมูลอยู่ที่เครื่องสแกนลายนิ้วมือ หรือไม่ 2) หากไม่มีข้อมูลสิทธิ์ของพนักงานดำเนินการส่งสิทธิ์ใหม่อีกครั้ง 3) ให้พนักงานทดลองการสแกนลายนิ้วมือเพื่อเข้างาน-ออกงานอีกครั้งที่เครื่องดังกล่าวที่แจ้งมา 4) หากสแกนลายนิ้วมือไม่ได้อีกต้องไปดูหน้างานว่าสภาพลายนิ้วมือเปลี่ยนแปลงจากเดิมต้องเก็บลายนิ้วมือใหม่อีกครั้งที่หน้าเครื่องสแกนลายนิ้วมือ

ขั้นตอน	ปัญหา/อุปสรรค	แนวทางแก้ไข
6) นำเข้าข้อมูลการลงเวลาปฏิบัติงาน	งานระบบ finger Scan นำเข้าข้อมูลไม่ครบทุกจุด	ดำเนินการนำเข้าข้อมูลอีกครั้งให้ครบทุกจุด
7) รายงานการลงเวลาปฏิบัติงาน	พนักงานแจ้งว่า ข้อมูลรายงานการมาปฏิบัติงานไม่ถูกต้อง	1) ให้พนักงานเข้าไปสืบค้นข้อมูลการลงเวลาจากระบบสารสนเทศบริหารงานบุคคล 2) ให้พนักงานตรวจดูว่าข้อมูลการลงเวลานั้น เป็นเวลาเข้างาน หรือออกงานที่ถูกต้องหรือไม่ 3) ให้พนักงานดูว่าข้อมูลรายงานการมาปฏิบัติงาน 1 วัน ที่ถูกต้องนั้นจะต้องประกอบด้วยการสแกนลายนิ้วมือเพื่อเข้างาน 1 ครั้งและเพื่อออกงาน 1 ครั้ง 4) พนักงานสามารถดูรายงานการมาปฏิบัติงานย้อนหลังเป็นรายเดือนได้

5.2 ข้อเสนอแนะ

เพื่อให้การปฏิบัติงานแทนกันสามารถทำงานให้เป็นไปอย่างมีประสิทธิภาพ เกิดประโยชน์กับผู้รับบริการมากที่สุด ผู้เขียนได้นำข้อค้นพบจากการปฏิบัติงานมาเป็นแนวทางในการพัฒนางานและมีข้อเสนอแนะ โดยแบ่งเป็นประเด็น ดังนี้

หากผู้ปฏิบัติงานตรวจสอบรายละเอียดการทำงานในขั้นตอนที่ (1) นำเข้าข้อมูลพนักงานใหม่ และขั้นตอนที่ (2) ตรวจสอบพร้อมปรับแก้ข้อมูลให้ถูกต้อง โดยไม่มีข้อผิดพลาดตั้งแต่ต้นทาง การดำเนินการในขั้นตอนที่ (3) กำหนดสิทธิ์ให้กับพนักงานใหม่ และขั้นตอนที่ (4) ส่งข้อมูลสิทธิ์ให้กับพนักงานใหม่ จะเป็นประโยชน์ ดังนี้

(1) เป็นการลดภาระงาน สามารถทำให้พนักงานใหม่ได้ใช้งานจริงภายในวันที่มารายงานตัวเข้าทำงานทันที

(2) ช่วยลดเวลา สามารถทำให้พนักงานใหม่ได้ใช้งานจริงภายใน 2 นาที หลังจากทำการส่งข้อมูลสิทธิ์ไปที่เครื่องสแกนลายนิ้วมือ

(3) การได้ใช้ทรัพยากรข้อมูลการลงเวลาปฏิบัติงานให้เกิดประโยชน์มากที่สุดกับมหาวิทยาลัย มีรายงานที่เป็นการประมวลผลในลักษณะตัวบุคคลเป็นรายวัน รายเดือน และรายปีแล้วนั้น น่าจะมีรายงานเสนอต่อผู้บริหารเพื่อประกอบการตัดสินใจที่เป็นลักษณะวิเคราะห์การมาทำงานที่ตรงต่อเวลาเป็นรายงานหน่วยงาน เช่น รายงานแยกเป็นแต่ละฝ่าย รายงานแยกเป็นแต่ละงาน หรือรายงานแยกตามอายุการทำงาน เป็นต้น

สำหรับส่วนท้ายของข้อเสนอแนะอยากเพิ่มเติมให้ทราบว่ามี application บนสมาร์ตโฟนที่เริ่มนำมาใช้งานสำหรับการเช็คอินเวลาพร้อมใบหน้า ระบุพิกัด เพื่อการลงเวลาปฏิบัติงาน เช่น TimeMint Jarviz iWORK SmartTA OneDee.ai HappyWork เป็นต้น หากในภายภาคหน้าจะประยุกต์ใช้การเช็คอินผ่านสมาร์ตโฟนด้วย Application Timestamp Camera เพื่อการเช็คอินเวลาและภาพถ่ายแทนการสแกนลายนิ้วมือก็น่าจะเป็นการประหยัดต้นทุนให้กับมหาวิทยาลัยได้

บรรณานุกรม

ชัยรัตน์ องค์วิศิษฐ์. (2548). *ระบบตรวจสอบลายนิ้วมือแบบอัตโนมัติเพื่อประมวลผลบนสมาร์ตคาร์ด.* (วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย).

ธนาคารแห่งประเทศไทย. (2563). *แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ*. สืบค้นจาก https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2563/ThaiPDF/25630177.pdf

พิทย์พิมล ชูรอด, เนาวลักษณ์ แสงสนิท และ สุพิริยา ผลนาค. (2557). *ระบบยืมหนังสือด้วยเครื่องสแกนลายนิ้วมือของสำนักหอสมุดมหาวิทยาลัยทักษิณ วิทยาเขตพัทลุง*. สืบค้นจาก https://pulinet.oas.psu.ac.th › article › download

พลากร ป้องกัน และ วีรวัฒน์ บุญโต. (2561). *ระบบตรวจสอบการเข้าเรียนแบบเวลาจริงด้วยลายนิ้วมือ*. สืบค้นจาก http://digital_collect.lib.buu.ac.th/project/b00257449.pdf

มหาวิทยาลัยวลัยลักษณ์ ส่วนทรัพยากรมนุษย์และองค์กร. (2565). *ข้อมูลบุคลากร*. สืบค้นจาก https://hro.wu.ac.th/personnel_info/

มหาวิทยาลัยวลัยลักษณ์ ส่วนแผนงานและยุทธศาสตร์. (2560). *แผนยุทธศาสตร์ 20 ปี*. นครศรีธรรมราช: กรีนโซน.

มหาวิทยาลัยวลัยลักษณ์ ศูนย์เทคโนโลยีดิจิทัล. (2564). *แผนพัฒนาเทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์ ระยะเวลา 4 ปี*. สืบค้นจาก https://cdt.wu.ac.th/?page_id=13409&lang=th

สมทรง ณ นคร, วิชุดา ไชยศิวามงคล, นิยะดา ห่อนาค, สุพรรณี อึ้งปัญสัตวงศ์, อำนวย มณีศรีวงศ์กูล, รัศมี สุวรรณวีระกำธร และ กุสุมา ชูศิลป์. (2554) ความสัมพันธ์ระหว่างแบบลายนิ้วมือและพหุปัญญา. *วารสารวิจัย มข*, *16*(8), 951-964.

สำนักงานพัฒนารัฐบาลดิจิทัล. (2564). *มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐสำหรับบุคคลธรรมดาที่มีสัญชาติไทย (Digital ID)(มรด.1-1:2564 และ มรด.1-2:2564)*. สืบค้นจาก https://standard.dga.or.th/wp-content/uploads/2021/09/3.Digital-ID-DGS-1-2_2564.pdf

สำรวน เวียงสมุทร. (2554). *การระบุบุคคลด้วยไบโอเมตริกซ์*. สืบค้นจาก https://www.thaiscience.info/Journals/Article/JSMU/10888194.pdf

อรรถพล ศิลปะกิจโกศล, ชาญณรงค์ ประกอบดี และ ภูริทัต สุธรรมมา. (2553). *เครื่องสแกนลายนิ้วมือเพื่อเปิด-ปิดประตู*. สืบค้นจาก http://sutir.sut.ac.th:8080/sutir/handle/123456789/7304

ภาคผนวก

ภาคผนวก 1 ประกาศมหาวิทยาลัยวลัยลักษณ์เรื่องการลงเวลาปฏิบัติงานของพนักงานและลูกจ้าง มหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๑

ภาคผนวก 2 ประกาศมหาวิทยาลัยวลัยลักษณ์เรื่องกำหนดเกณฑ์การมาสายของพนักงานและลูกจ้าง มหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕

ภาคผนวก 3 ระเบียบมหาวิทยาลัยวลัยลักษณ์ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา มหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๓

ภาคผนวก 4 ประกาศที่ ธปท.ฝทง.ว.760/2563 เรื่อง นำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ(Biometric Technology) ในการให้บริการทางการเงิน ลงวันที่ 22 กรกฎาคม 2563

ภาคผนวก 5 มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่อง การใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ เกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (DIGITALIZATION: DIGITAL ID - IDENTITY PROOFING AND AUTHENTICATION) พ.ศ. ๒๕๖๔

ภาคผนวก 6 ข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยประมวลจริยธรรมและธรรมาภิบาล นายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕

ภาคผนวก 1 ประกาศมหาวิทยาลัยวลัยลักษณ์
เรื่องการลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๑

ประกาศมหาวิทยาลัยวลัยลักษณ์
เรื่อง การลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๑

.....

อนุสนธิประกาศมหาวิทยาลัยวลัยลักษณ์ ลงวันที่ ๕ มิถุนายน พ.ศ.๒๕๖๐ ได้ประกาศการลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ.๒๕๖๐ ไปแล้ว นั้น

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ให้มีความชัดเจนและเหมาะสมยิ่งขึ้น อาศัยอำนาจตามความในมาตรา ๒๔ แห่งพระราชบัญญัติมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๓๕ ประกอบกับข้อ ๗ แห่งระเบียบมหาวิทยาลัยวลัยลักษณ์ว่าด้วยการลาของพนักงานและลูกจ้าง พ.ศ. ๒๕๓๕ จึงให้ยกเลิกประกาศฉบับดังกล่าวข้างต้น และให้ใช้แนวปฏิบัติดังนี้

ข้อ ๑ การลงเวลาปฏิบัติงานของพนักงานและลูกจ้าง ให้ถือปฏิบัติตามระเบียบมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา พ.ศ. ๒๕๔๓ หรือฉบับอื่นที่มีการปรับปรุงใหม่

ข้อ ๒ ให้พนักงานและลูกจ้างลงเวลาปฏิบัติงาน และไม่ลงเวลาปฏิบัติงานตามลักษณะงานและหน้าที่ความรับผิดชอบ ดังนี้

๒.๑ พนักงานหรือลูกจ้างที่ต้องลงเวลาปฏิบัติงาน ได้แก่ พนักงานหรือลูกจ้างสายปฏิบัติการวิชาชีพและบริหารทั่วไป ที่มีหน้าที่และความรับผิดชอบ ต้องอยู่ปฏิบัติงานประจำ เพื่อให้บริการด้านวิชาชีพ หรือด้านวิชาการ หรืออื่นๆ ที่เป็นงานสนับสนุนทั่วไป ได้แก่

(๑) กลุ่มตำแหน่งปฏิบัติการวิชาชีพและบริหารทั่วไป

(๒) กลุ่มตำแหน่งบริหารจัดการ ประกอบด้วย หัวหน้างาน หัวหน้าฝ่าย หัวหน้าสำนักงาน (เป็นตำแหน่งที่เทียบเท่าหัวหน้าฝ่ายสังกัดศูนย์/สถาบัน) หรือตำแหน่งอื่นที่เทียบเท่า ตามที่มหาวิทยาลัยกำหนด ซึ่งพนักงานกลุ่มนี้ยังมีภาระหน้าที่งานบริการที่ต้องปฏิบัติด้วย

๒.๒ พนักงานหรือลูกจ้างที่ไม่ต้องลงเวลาปฏิบัติงาน เนื่องจากเป็นงานลักษณะที่มีหน้าที่และความรับผิดชอบไม่ได้ใช้ระยะเวลาการปฏิบัติงานในเวลาปกติของมหาวิทยาลัย และกรณีเป็นตำแหน่งบริหารต้องรับผิดชอบงานตลอด ๒๔ ชั่วโมง ได้แก่

(๑) พนักงานสายบริหารวิชาการ

(๒) พนักงานสายวิชาการ

(๓) พนักงานสายปฏิบัติการวิชาชีพและบริหารทั่วไป กลุ่มตำแหน่งบริหารจัดการ ระดับหัวหน้าส่วน หัวหน้าหน่วย หัวหน้าสำนักงาน ผู้จัดการโครงการ หรือตำแหน่งอื่นที่เทียบเท่า ซึ่งเป็นผู้บังคับบัญชาระดับหัวหน้าหน่วยงาน

ข้อ ๓ ให้พนักงานหรือลูกจ้างที่ต้องลงเวลาปฏิบัติงานตามข้อ ๒.๑ บันทึกเวลาเข้าและออกการปฏิบัติงานด้วยการสแกนลายนิ้วมือ หรือตามระบบที่มหาวิทยาลัยกำหนด และให้ผู้บังคับบัญชาของหน่วยงานเป็นผู้ควบคุมการลงเวลาปฏิบัติงาน

ข้อ ๔ กรณีพนักงานหรือลูกจ้างตามข้อ ๒.๑ ไม่ลงเวลาปฏิบัติงาน ถือว่าเป็นการฝ่าฝืนไม่ปฏิบัติตามนโยบาย ข้อบังคับ ระเบียบ และธรรมเนียมปฏิบัติที่มหาวิทยาลัยกำหนดอาจมีความผิดทางวินัย

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๕ ธันวาคม พ.ศ. ๒๕๖๑

(ศาสตราจารย์ ดร.สมบัติ ธำรงธัญวงศ์)
อธิการบดีมหาวิทยาลัยวลัยลักษณ์

ภาคผนวก 2 ประกาศมหาวิทยาลัยวลัยลักษณ์
เรื่องกำหนดเกณฑ์การมาสายของพนักงานและลูกจ้าง มหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕

ประกาศมหาวิทยาลัยวลัยลักษณ์

เรื่อง กำหนดเกณฑ์การมาสายของพนักงานและลูกจ้าง มหาวิทยาลัยวลัยลักษณ์

พ.ศ. ๒๕๖๕

.....

อนุสนธิประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง กำหนดเกณฑ์การมาสายของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๔ ฉบับลงวันที่ ๑๘ กุมภาพันธ์ พ.ศ. ๒๕๖๔ ได้กำหนดเกณฑ์การมาสายของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ ไปแล้ว นั้น

เนื่องจากประกาศดังกล่าวถือปฏิบัติมาแล้วเป็นเวลา ๑ ปี พบว่ามีพนักงานที่มาปฏิบัติงานสายหรือออกก่อนจะเลี่ยงไม่ลงเวลาปฏิบัติงาน เพื่อเป็นการรณรงค์ส่งเสริมให้พนักงานปฏิบัติงานด้วยความซื่อสัตย์สุจริต ตรงต่อเวลาและรักษาระเบียบวินัยการปฏิบัติงานอย่างเคร่งครัด อันจะส่งผลดีต่อวัฒนธรรมองค์กร มหาวิทยาลัยจึงเห็นสมควรปรับเกณฑ์ในข้อ ๒ ให้มีความเหมาะสมยิ่งขึ้น อาศัยอำนาจตามความในมาตรา ๒๔ แห่งพระราชบัญญัติมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๓๕ ข้อ ๗ ของระเบียบมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการจัดวันเวลาทำงานและการทำงานล่วงเวลา พ.ศ. ๒๕๖๓ และข้อ ๗ ของระเบียบมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการลาของพนักงานและลูกจ้าง พ.ศ. ๒๕๓๕ จึงให้ยกเลิกประกาศฉบับอนุสนธิดังกล่าว และให้ใช้แนวปฏิบัติ ดังนี้

ข้อ ๑ พนักงานและลูกจ้างที่ต้องลงเวลาปฏิบัติงาน ตามประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง การลงเวลาปฏิบัติงานของพนักงานและลูกจ้างมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๑ ฉบับลงวันที่ ๑๔ ธันวาคม พ.ศ. ๒๕๖๑ ต้องลงเวลาปฏิบัติงานตามเวลาที่กำหนด ยกตัวอย่างเวลาปฏิบัติงาน ดังนี้

เวลาทำงาน	ลงเวลาเข้า	ลงเวลาออก
๐๘.๓๐ - ๑๖.๓๐ น.	ภายในเวลา ๐๘.๓๐ น. หากลงเวลาหลัง ๐๘.๓๐ น. ถือว่ามาสาย	หลังเวลา ๑๖.๓๐ น. หากลงเวลาก่อน ๑๖.๓๐ น. ถือว่าออกก่อน
๐๘.๐๐ - ๑๖.๐๐ น.	ภายในเวลา ๐๘.๐๐ น. หากลงเวลาหลัง ๐๘.๐๐ น. ถือว่ามาสาย	หลังเวลา ๑๖.๐๐ น. หากลงเวลาก่อน ๑๖.๐๐ น. ถือว่าออกก่อน
๑๔.๐๐ - ๒๒.๐๐ น.	ภายในเวลา ๑๔.๐๐ น. หากลงเวลาหลัง ๑๔.๐๐ น. ถือว่ามาสาย	หลังเวลา ๒๒.๐๐ น. หากลงเวลาก่อน ๒๒.๐๐ น. ถือว่าออกก่อน

การลาครึ่งวัน ต้องลงเวลาปฏิบัติงานตามเวลาที่กำหนด ยกตัวอย่างเวลาปฏิบัติงาน ดังนี้

เวลาทำงาน	การลา	ลงเวลาเข้า	ลงเวลาออก
๐๘.๓๐-๑๖.๓๐ น.	ลาครึ่งวันเช้า เข้าทำงานครึ่งวันบ่าย	ภายในเวลา ๑๓.๐๐ น. หากลงเวลาหลัง ๑๓.๐๐ น. ถือว่ามาสาย	หลังเวลา ๑๖.๓๐ น. หากลงเวลาก่อน ๑๖.๓๐ น. ถือว่าออกก่อน
๐๘.๓๐-๑๖.๓๐ น.	ลาครึ่งวันบ่าย เข้าทำงานครึ่งวันเช้า	ภายในเวลา ๐๘.๓๐ น. หากลงเวลาหลัง ๐๘.๓๐ น. ถือว่ามาสาย	หลังเวลา ๑๒.๐๐ น. หากลงเวลาก่อน ๑๒.๐๐ น. ถือว่าออกก่อน
๐๘.๐๐-๑๖.๐๐ น.	ลาครึ่งวันเช้า เข้าทำงานครึ่งวันบ่าย	ภายในเวลา ๑๒.๓๐ น. หากลงเวลาหลัง ๑๒.๓๐ น. ถือว่ามาสาย	หลังเวลา ๑๖.๐๐ น. หากลงเวลาก่อน ๑๖.๐๐ น. ถือว่าออกก่อน
๐๘.๐๐-๑๖.๐๐ น.	ลาครึ่งวันบ่าย เข้าทำงานครึ่งวันเช้า	ภายในเวลา ๐๘.๐๐ น. หากลงเวลาหลัง ๐๘.๐๐ น. ถือว่ามาสาย	หลังเวลา ๑๑.๓๐ น. หากลงเวลาก่อน ๑๑.๓๐ น. ถือว่าออกก่อน
๑๔.๐๐-๒๒.๐๐ น.	ลาครึ่งวันเช้า เข้าทำงานครึ่งวันบ่าย	ภายในเวลา ๑๘.๓๐ น. หากลงเวลาหลัง ๑๘.๓๐ น. ถือว่ามาสาย	หลังเวลา ๒๒.๐๐ น. หากลงเวลาก่อน ๒๒.๐๐ น. ถือว่าออกก่อน
๑๔.๐๐-๒๒.๐๐ น.	ลาครึ่งวันบ่าย เข้าทำงานครึ่งวันเช้า	ภายในเวลา ๑๔.๐๐ น. หากลงเวลาหลัง ๑๔.๐๐ น. ถือว่ามาสาย	หลังเวลา ๑๗.๓๐ น. หากลงเวลาก่อน ๑๗.๓๐ น. ถือว่าออกก่อน

ข้อ ๒ กรณีพนักงานและลูกจ้างไม่ลงเวลาเข้าหรือออกจากการทำงานให้ถือเป็นการมาสาย รวมถึงการออกก่อนก็ให้นับเป็นการมาสายเช่นเดียวกัน

ข้อ ๓ การมาสายให้นำไปพิจารณาประเมินผลการปฏิบัติงานในเรื่องความตั้งใจ ทุ่มเท การปฏิบัติงาน การตรงต่อเวลา โดยให้อยู่ในดุลยพินิจของผู้บังคับบัญชา และกรณีมาสายเกิน ๑๒ ครั้ง จะไม่ได้รับการขึ้นเงินเดือนประจำปีในปีงบประมาณนั้น ๆ

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ ๑ มีนาคม พ.ศ.๒๕๖๕ เป็นต้นไป

ประกาศ ณ วันที่ ๗ มีนาคม พ.ศ. ๒๕๖๕

(ศาสตราจารย์ ดร.สมบัติ ธำรงธัญวงศ์)

รักษาการแทนอธิการบดีมหาวิทยาลัยวลัยลักษณ์

๗ มี.ค. ๖๕ เวลา ๑๕:๓๖:๕ Personal PKI-LN

Signature Code : g09ql-TQxXK-8r5nC-E8kRw

ภาคผนวก 3 ระเบียบมหาวิทยาลัยวลัยลักษณ์
ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา มหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๓

ระเบียบมหาวิทยาลัยวลัยลักษณ์
ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา
พ.ศ. ๒๕๖๓

.....

โดยที่เป็นการสมควรปรับปรุงระเบียบมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา ให้มีความเหมาะสมสอดคล้องกับสภาวการณ์ปัจจุบัน และเป็นการส่งเสริมพัฒนาระบบการบริหารงานบุคคลให้มีประสิทธิภาพยิ่งขึ้น ฉะนั้น อาศัยอำนาจตามความในมาตรา ๑๖ (๒) และ (๙) แห่งพระราชบัญญัติมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๓๕ ข้อ ๔๓ แห่งข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการบริหารงานบุคคล พ.ศ. ๒๕๖๑ ประกอบกับมติคณะกรรมการบริหารงานบุคคล ในการประชุมครั้งที่ ๕/๒๕๖๓ เมื่อวันที่ ๓๐ กรกฎาคม ๒๕๖๓ มติคณะกรรมการการเงินและทรัพย์สิน ในการประชุมครั้งที่ ๔/๒๕๖๓ เมื่อวันที่ ๒๐ สิงหาคม ๒๕๖๓ และมติสภามหาวิทยาลัยวลัยลักษณ์ ในการประชุมครั้งที่ ๖/๒๕๖๓ เมื่อวันที่ ๑๒ กันยายน ๒๕๖๓ จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา พ.ศ. ๒๕๖๓”

ข้อ ๒ ให้ใช้ระเบียบนี้ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๓ เป็นต้นไป

บรรดาระเบียบ หรือประกาศอื่นใดในส่วนที่มีบัญญัติไว้ในระเบียบนี้ ซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๓ ให้ยกเลิก

(๑) ระเบียบมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการจัดเวลาทำงานและการทำงานล่วงเวลา พ.ศ. ๒๕๔๓

(๒) ประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง ค่าใช้จ่ายในการเดินทางปฏิบัติงาน กรณีการปฏิบัติงานล่วงเวลา พ.ศ. ๒๕๕๗

(๓) ประกาศมหาวิทยาลัยลักษณ์ เรื่อง ค่าตอบแทนผู้ปฏิบัติงานล่วงเวลา กรณีผู้ปฏิบัติงานบริการห้องสมุด ช่วง ๓ สัปดาห์ก่อนการสอบปลายภาคและช่วงสอบปลายภาค ปฏิบัติงานเวลา ๒๐.๓๐ - ๒๔.๐๐ น. พ.ศ. ๒๕๕๗

(๔) ประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง ค่าตอบแทนพนักงานเวรฉุกเฉิน และขับรถพยาบาลของมหาวิทยาลัย พ.ศ. ๒๕๔๙

ข้อ ๔ ในระเบียบนี้

“มหาวิทยาลัย”	หมายถึง	มหาวิทยาลัยวลัยลักษณ์
“อธิการบดี”	หมายถึง	อธิการบดีมหาวิทยาลัยวลัยลักษณ์

“พนักงาน”	หมายถึง	พนักงาน ลูกจ้างประจำ ลูกจ้างชั่วคราวรายเดือน และลูกจ้างชั่วคราวรายวันของมหาวิทยาลัย วลัยลักษณ์
“ลูกจ้างชั่วคราวรายเดือน”	หมายถึง	บุคคลที่มหาวิทยาลัยจ้างให้ปฏิบัติงานที่มีลักษณะเป็นการชั่วคราว กำหนดเวลาการจ้างเป็นรายเดือน
“ลูกจ้างชั่วคราวรายวัน”	หมายถึง	บุคคลที่มหาวิทยาลัยจ้างให้ปฏิบัติงานที่มีลักษณะเป็นการชั่วคราว กำหนดเวลาการจ้างเป็นรายวัน
“วันทำการปกติ”	หมายถึง	วันจันทร์ถึงวันศุกร์ หรือวันอื่นใดที่มหาวิทยาลัยกำหนดขึ้นให้เป็นวันทำการปกติตามความเหมาะสมตามลักษณะของงาน
“เวลาทำงานปกติ”	หมายถึง	เวลาทำงานของมหาวิทยาลัย ระหว่างเวลา ๐๘.๓๐ - ๑๖.๓๐ น. ของวันทำการปกติ หรือเวลาอื่นใดที่กำหนดให้เป็นเวลาทำงานปกติ
“การจัดเวลาทำงาน”	หมายถึง	การจัดเวลาทำงานของพนักงานที่มีระยะเวลาการปฏิบัติงานแน่นอนนอกเหนือจากเวลาทำงานปกติ
“การทำงานล่วงเวลา”	หมายถึง	การทำงานเกินกว่าเวลาทำงานปกติที่มหาวิทยาลัยกำหนด หรือเกินกว่าเวลาทำงานที่ได้รับอนุมัติการจัดเวลาทำงาน การทำงานในวันหยุดประจำสัปดาห์ การทำงานในวันหยุดประจำปี ตามประกาศของมหาวิทยาลัย
“ค่าล่วงเวลา”	หมายถึง	เงินค่าจ้างที่มหาวิทยาลัยจ่ายให้แก่พนักงานและลูกจ้าง นอกเหนือจากเงินเดือนหรือค่าจ้าง เพื่อตอบแทนการทำงานล่วงเวลานอกเหนือจากวันเวลาทำงานปกติ
“วันหยุดประจำสัปดาห์”	หมายถึง	วันเสาร์และวันอาทิตย์ หรือวันอื่นใดที่มหาวิทยาลัยกำหนดขึ้นเพื่อความเหมาะสมตามลักษณะของงาน
“วันหยุดประจำปี”	หมายถึง	วันหยุดที่มหาวิทยาลัยประกาศให้เป็นวันหยุดประจำปี
“วันหยุดพิเศษ”	หมายถึง	วันหยุดที่ทางราชการประกาศเป็นวันหยุดราชการนอกจากวันหยุดประจำสัปดาห์ และวันหยุดประจำปี
“หน่วยงาน”	หมายถึง	สำนักงานอธิการบดี สำนักวิชา ศูนย์ สถาบัน หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะ

เทียบเท่าสำนักงานอธิการบดี สำนักวิชา ศูนย์หรือสถาบัน หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าส่วนงาน ยกเว้นหน่วยงานที่มีลักษณะเฉพาะที่ได้รับอนุมัติจากมหาวิทยาลัยเป็นกรณีไป

ข้อ ๕ ให้อธิการบดีรักษาการให้เป็นไปตามระเบียบนี้ และมีอำนาจวินิจฉัยชี้ขาด คำวินิจฉัยของอธิการบดีให้ถือเป็นที่สุด รวมทั้งมีอำนาจออกประกาศโดยความเห็นชอบของคณะกรรมการบริหารงานบุคคลเพื่อกำหนดหลักเกณฑ์ และวิธีการเพื่อปฏิบัติตามระเบียบนี้

ข้อ ๖ ให้อธิการบดี หรือผู้ที่อธิการบดีมอบหมาย เป็นผู้มีอำนาจสั่ง หรืออนุมัติการทำงานล่วงเวลา และอนุมัติการจัดเวลาทำงานพนักงาน

หมวด ๑
การจัดวันและเวลาทำงาน

ข้อ ๗ กรณีที่ไม่สามารถจัดเวลาทำงานของพนักงานได้ตามเวลาทำงานปกติ แต่เป็นงานที่มีระยะเวลาการปฏิบัติงานแน่นอน อาทิ ตารางการให้บริการ ตารางการตรวจซ่อมบำรุง ตารางการตรวจตรารักษาความปลอดภัย ฯลฯ ให้ใช้หลักเกณฑ์สำหรับการจัดเวลาทำงาน ดังนี้

(๑) ให้จัดการทำงานเป็นกะ สำหรับงานที่มีลักษณะปฏิบัติงานต่อเนื่องต้องปฏิบัติงานไม่น้อยกว่า ๑๖ ชั่วโมง โดยให้หัวหน้าหน่วยงานกำหนดการทำงานเป็นกะได้ตามความเหมาะสม อาทิ การปฏิบัติงาน ๑๖ ชั่วโมง ให้จัดเป็น ๒ กะ หรือ ๒๔ ชั่วโมงให้จัดเป็น ๓ กะ

(๒) ให้จัดตารางทำงานแบบเหลื่อมเวลา สำหรับงานที่มีลักษณะภาระงานอาจจะมากในช่วงเวลาหนึ่ง และน้อยในอีกช่วงเวลาหนึ่ง หรือต้องให้บริการเกินเวลาทำการปกติ โดยให้หัวหน้าหน่วยงานวิเคราะห์ แล้วกำหนดให้พนักงานปฏิบัติงาน (เข้าปฏิบัติงาน - เลิกปฏิบัติงาน) ต่างเวลากัน โดยให้มีเวลาทำงาน ๘ ชั่วโมงต่อวัน (รวมเวลาหยุดพักหนึ่งชั่วโมง) อาทิ ๐๗.๓๐ - ๑๕.๓๐ น. หรือ ๐๘.๓๐ - ๑๖.๓๐ น. หรือ ๑๒.๐๐ - ๒๐.๐๐ น.ฯลฯ โดยถือว่าการปฏิบัติงานในช่วงเวลาที่หัวหน้าหน่วยงานกำหนดเป็นการปฏิบัติงานในเวลาทำงานปกติ

(๓) ให้จัดตารางวันหยุดที่ไม่เหมือนกัน สำหรับงานที่กำหนดให้มีตารางการทำงานในวันหยุดประจำสัปดาห์ (เสาร์หรืออาทิตย์) ให้หัวหน้าหน่วยงานกำหนดให้พนักงานที่ต้องปฏิบัติงานในวันหยุดดังกล่าว ได้มีวันหยุดทดแทนในวันอื่นให้ครบจำนวน ๒ วันต่อสัปดาห์ อาทิ หยุดวันศุกร์ - เสาร์ หรือ อาทิตย์ - จันทร์ หรือหยุดในวันอื่นที่หัวหน้าหน่วยงานเห็นสมควร

ข้อ ๘ การทำงานล่วงเวลาจะกระทำได้ในเงื่อนไข ดังต่อไปนี้

(๑) ต้องเป็นงานซึ่งไม่สามารถปฏิบัติได้แล้วเสร็จภายในเวลาที่กำหนด และจำเป็นต้องปฏิบัติให้เสร็จเรียบร้อยโดยเร็วเพื่อประโยชน์ และเพื่อป้องกันมิให้เสียหายแก่มหาวิทยาลัย หรือเป็นงานที่ไม่สามารถปฏิบัติได้ในเวลาทำงานโดยปกติ หรือไม่สามารถปฏิบัติได้ตามเวลาที่ได้รับอนุมัติการจัดเวลาทำงาน

(๒) การทำงานในเวลาทำงานปกติ และการทำงานล่วงเวลาต่อเนื่องกัน ต้องไม่เกิน ๑๒ ชั่วโมง (เวลาทำงานปกติ ๘ ชั่วโมง และการทำงานล่วงเวลาต่อเนื่องต้องไม่เกิน ๔ ชั่วโมง) รวมเวลา

หยุดพักหนึ่งชั่วโมง ทั้งนี้เศษนาทีของชั่วโมงตั้งแต่ ๓๐ นาที ขึ้นไป ให้นับเป็น ๑ ชั่วโมง และหากน้อยกว่า ๓๐ นาที ลงมาให้ตัดทิ้ง

ในกรณีมีเหตุเร่งด่วนพิเศษ ให้เสนอขออนุมัติจากรองอธิการบดีที่กำกับดูแลพิจารณาเป็นกรณีไป

(๓) การทำงานล่วงเวลาในวันหยุดประจำสัปดาห์ วันหยุดประจำปี หรือวันหยุดพิเศษต้องไม่เกิน ๘ ชั่วโมง รวมเวลาหยุดพักหนึ่งชั่วโมง

ในกรณีมีเหตุเร่งด่วนพิเศษ ให้เสนอขออนุมัติจากรองอธิการบดีที่กำกับดูแลพิจารณาเป็นกรณีไป

หมวด ๒
การขออนุมัติทำงานล่วงเวลา

ข้อ ๙ การทำงานล่วงเวลาต้องได้รับคำสั่ง หรือได้รับการอนุมัติจากผู้มีอำนาจตามข้อ ๖ ก่อน เว้นแต่กรณีมีความจำเป็นเร่งด่วน จะทำงานล่วงเวลาไปก่อนก็ได้ แต่ต้องรายงานให้ผู้ที่มีอำนาจอนุมัติทราบเพื่อขออนุมัติการทำงานล่วงเวลาดังกล่าวในโอกาสแรกที่สามารถทำได้

ข้อ ๑๐ การขออนุมัติ การรายงานการทำงานล่วงเวลา การเบิกค่าล่วงเวลา และการหยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลา ให้เป็นไปตามแบบที่มหาวิทยาลัยกำหนด

ข้อ ๑๑ การขออนุมัติการทำงานล่วงเวลา หัวหน้าหน่วยงานต้องวางแผนการทำงานล่วงเวลาและขออนุมัติการทำงานล่วงเวลาล่วงหน้า กรณีมีความจำเป็น หรือเร่งด่วนสามารถขออนุมัติการทำงานย้อนหลังได้ ไม่เกิน ๕ วันทำการ โดยเสนอต่อรองอธิการบดีที่กำกับดูแลพิจารณาอนุมัติ

หมวด ๓
อัตราค่าตอบแทนและอัตราค่าเดินทางการทำงานล่วงเวลา

ข้อ ๑๒ พนักงานที่ไม่มีสิทธิได้รับเงินค่าล่วงเวลา หรือหยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลาตามระเบียบนี้ ได้แก่

(๑) พนักงานสายบริหารวิชาการ และพนักงานสายวิชาการ

(๒) พนักงานสายปฏิบัติการวิชาชีพและบริหารทั่วไป กลุ่มตำแหน่งบริหารจัดการ ตั้งแต่ระดับหัวหน้างาน หัวหน้าฝ่าย หัวหน้าส่วน หรือเทียบเท่าขึ้นไป

(๓) พนักงานที่ได้รับค่าตอบแทนในลักษณะเหมาจ่ายเป็นรายเดือน

(๔) ตำแหน่งอื่นตามที่มหาวิทยาลัยกำหนด

ข้อ ๑๓ พนักงานที่ทำงานล่วงเวลา โดยใช้สิทธิขอเบิกค่าล่วงเวลา ให้ได้รับค่าล่วงเวลาในอัตราชั่วโมงละ ๕๐ บาท

ข้อ ๑๔ พนักงานที่ทำงานล่วงเวลา กรณีปฏิบัติงานบริการห้องสมุด ช่วง ๓ สัปดาห์สุดท้ายก่อนการสอบปลายภาค และช่วงสอบปลายภาค ปฏิบัติงานเวลา ๒๐.๓๐ - ๒๔.๐๐ น. ให้ได้รับค่าล่วงเวลาในอัตราเหมาจ่ายคนละ ๒๕๐ บาท ทั้งนี้ สิทธิการเบิกค่าเดินทางในการปฏิบัติงานล่วงเวลาให้เป็นไปตามข้อ ๑๖

ข้อ ๑๕ พนักงานที่เข้าเวรฉุกเฉินนอกเวลางานปกติ หรือวันหยุดประจำสัปดาห์ วันหยุดประจำปี หรือวันหยุดพิเศษ เช่น งานตรวจสอบเฝ้าระวังระบบไฟฟ้าและน้ำประปา ปฏิบัติงานไม่น้อยกว่า ๘ ชั่วโมง (รวมเวลาหยุดพักหนึ่งชั่วโมง) หรือตามระยะเวลาที่หน่วยงานกำหนด ให้ได้รับค่าล่วงเวลาในอัตราเหมาจ่ายคนละ ๓๕๐ บาท โดยรวมค่าเดินทางการทำงานล่วงเวลาแล้ว

ข้อ ๑๖ พนักงานที่ทำงานล่วงเวลา โดยใช้สิทธิรับเงินค่าล่วงเวลา หรือใช้สิทธิขอหยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลา มหาวิทยาลัยจะให้สิทธิเบิกค่าใช้จ่ายในการเดินทางปฏิบัติงานล่วงเวลาแทนการจัดรถบริการรับส่งพนักงานของมหาวิทยาลัย เฉพาะพนักงานที่ไม่พักในมหาวิทยาลัย ดังนี้

สถานที่ปฏิบัติงาน	อัตราค่าเดินทางการทำงานล่วงเวลา (บาท/ครั้ง)
๑. ปฏิบัติงาน ณ มหาวิทยาลัยวลัยลักษณ์ จังหวัดนครศรีธรรมราช	
๑.๑ เขตพื้นที่อำเภอท่าศาลา	๑๐๐
๑.๒ เขตนอกพื้นที่อำเภอท่าศาลา	๒๐๐
๒. ปฏิบัติงาน ณ ศูนย์วิทยบริการ จังหวัดสุราษฎร์ธานี	๒๐๐
๓. ปฏิบัติงาน ณ หน่วยประสานงานมหาวิทยาลัยวลัยลักษณ์ กรุงเทพมหานคร	๓๐๐

ข้อ ๑๗ กรณีมีการเปลี่ยนแปลงอัตราค่าล่วงเวลา และค่าใช้จ่ายตามระเบียบนี้ รวมทั้งการกำหนดลักษณะงานพิเศษให้ทำเป็นประกาศของมหาวิทยาลัย โดยความเห็นชอบของคณะกรรมการบริหารงานบุคคล

หมวด ๔
การเบิกจ่ายค่าล่วงเวลา

ข้อ ๑๘ การเบิกจ่ายค่าล่วงเวลา ให้ดำเนินการเบิกจ่ายให้แล้วเสร็จภายในวันที่ ๑๐ ของเดือนถัดไป

ข้อ ๑๙ ห้ามมิให้เบิกจ่ายค่าล่วงเวลา หรือหยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลาสำหรับการทำงานล่วงเวลา ดังต่อไปนี้

(๑) การทำงานล่วงเวลาต่อเนื่องในคราวเดียวกันวันหนึ่งน้อยกว่าหนึ่งชั่วโมง

(๒) เวลาหยุดพักตามที่มหาวิทยาลัยกำหนด

(๓) การทำงานนอกสถานที่ ซึ่งมีสิทธิเบิกเป็นค่าใช้จ่ายในการเดินทางไปปฏิบัติงานได้

(๔) การทำงานล่วงเวลาซึ่งได้รับค่าตอบแทนอื่นใดแล้ว

ข้อ ๒๐ พนักงานที่ทำงานล่วงเวลา โดยใช้สิทธิขอหยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลา ให้ใช้แนวปฏิบัติ ดังต่อไปนี้

(๑) ให้ขออนุมัติทำงานล่วงเวลาต่ออธิการบดี หรือผู้ที่อธิการบดีมอบหมาย

(๒) บันทึกลงเวลาปฏิบัติงานนอกเวลา

(๓) ให้ขอหยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลาต่อหัวหน้าหน่วยงาน (ผู้มีอำนาจอนุญาตการลาของพนักงานและลูกจ้าง) เมื่อได้รับอนุญาตแล้วจึงจะหยุดงานได้ แต่การหยุดปฏิบัติงานฯ ดังกล่าวต้องไม่หยุดข้ามปีงบประมาณ และไม่ก่อให้เกิดความเสียหายต่อหน่วยงาน ทั้งนี้ มิให้สะสมวันที่ยังมิได้หยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลาสำหรับการทำงานล่วงเวลาในปีงบประมาณนั้น รวมเข้ากับปีงบประมาณต่อ ๆ ไป

เว้นแต่การทำงานล่วงเวลาในเดือนกันยายน ให้หยุดปฏิบัติงานแทนการรับเงินค่าล่วงเวลา สำหรับการทำงานล่วงเวลาได้ภายในเดือนตุลาคมของปีปฏิทินนั้น และมิให้นำวันที่ยังมิได้หยุดปฏิบัติงานฯ ในปีงบประมาณนั้น ไปคำนวณเป็นเงินเพื่อเบิกจ่าย

ประกาศ ณ วันที่ ๑๕ ตุลาคม พ.ศ. ๒๕๖๓

(ศาสตราจารย์ ดร.วิจิตร ศรีสอ้าน)
นายกสภามหาวิทยาลัยวลัยลักษณ์

ภาคผนวก 4 ประกาศที่ ธปท.ฝทง.ว.760/2563
เรื่อง นำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ(Biometric Technology) ในการให้บริการทางการเงิน
ลงวันที่ 22 กรกฎาคม 2563

ธนาคารแห่งประเทศไทย

22 กรกฎาคม 2563

เรียน ผู้จัดการ

สถาบันการเงินทุกแห่ง
ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับที่มิใช่สถาบันการเงินทุกแห่ง
บริษัทผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับที่มิใช่สถาบันการเงินทุกแห่ง

ที่ ธปท.ฝทง. ว. 760 /2563 เรื่อง นำส่งแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

ธนาคารแห่งประเทศไทย (ธปท.) ได้ออกแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน โดยมีวัตถุประสงค์เพื่อให้ผู้ให้บริการทางการเงินที่มีการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงิน ใช้อ้างอิงเป็นมาตรฐานเพื่อให้มั่นใจว่าการให้บริการที่เกี่ยวข้องกับเทคโนโลยีชีวมิติมีความมั่นคงปลอดภัย สอดคล้องกับมาตรฐานสากล ซึ่งจะช่วยยกระดับการให้บริการทางการเงินและก่อให้เกิดประโยชน์แก่ผู้ใช้บริการ

แนวปฏิบัตินี้ครอบคลุมหลักการพึงปฏิบัติที่สำคัญในการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงิน ตั้งแต่ระดับนโยบายขององค์กรไปจนถึงแนวทางดำเนินการและการบริหารความเสี่ยงในการใช้เทคโนโลยีชีวมิติตลอดทั้งวงจรชีวิต (life cycle) ของข้อมูล รวมถึงการคุ้มครองผู้ใช้บริการและปฏิบัติตามกฎหมายที่เกี่ยวข้อง และมีรายละเอียดมาตรฐานเชิงเทคนิคสำหรับการใช้เทคโนโลยีการเปรียบเทียบใบหน้า ซึ่งเป็นเทคโนโลยีหลักที่มีการใช้งานในภาคการเงินในปัจจุบัน โดย ธปท. ได้จัดทำแนวปฏิบัตินี้ขึ้นโดยอ้างอิงจากมาตรฐานสากล และการประเมินโครงการทดสอบการใช้เทคโนโลยีชีวมิติในกระบวนการรู้จักลูกค้าภายใต้ regulatory sandbox ทั้งนี้ ในระยะต่อไป หากมีการนำเทคโนโลยีชีวมิติในรูปแบบอื่นมาให้บริการ ธปท. จะพิจารณากำหนดมาตรฐานเชิงเทคนิคเพิ่มเติมเพื่อเป็นมาตรฐานที่ดีในการนำไปใช้ต่อไป

สำหรับผู้ให้บริการทางการเงินที่ประสงค์จะนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงิน ต้องปฏิบัติตามแนวทางดังนี้

1. ผู้ให้บริการทางการเงินต้องถือปฏิบัติตามแนวปฏิบัติฉบับนี้อย่างครบถ้วน โดยคำนึงถึงประสิทธิภาพความแม่นยำของเทคโนโลยีที่เลือกใช้ การรักษาความปลอดภัยของข้อมูลลูกค้า และการปฏิบัติตามกฎหมายที่เกี่ยวข้องโดยเฉพาะกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

2. ผู้ให้บริการทางการเงินที่มีความประสงค์จะประยุกต์ใช้เทคโนโลยีชีวมิติเพื่อเปรียบเทียบภาพใบหน้าของผู้ใช้บริการกับแหล่งข้อมูลที่เชื่อถือได้ (trusted source) ในกระบวนการรู้จักตัวตนลูกค้า ต้องทดสอบการใช้เทคโนโลยีดังกล่าวภายใต้ regulatory sandbox ของ ธปท. โดยต้องปฏิบัติตามเงื่อนไขการทดสอบที่กำหนดโดยครบถ้วนและได้รับอนุญาตจาก ธปท. ก่อนให้บริการในวงกว้าง

3. ผู้ให้บริการทางการเงินที่ผ่านการทดสอบภายใต้ regulatory sandbox ของ ธปท. แล้ว สามารถประยุกต์ใช้เทคโนโลยีชีวมิติภายใต้โครงการที่ผ่านการทดสอบแล้ว กับธุรกรรมการเปิดบัญชีเงินฝาก การเปิดใช้บริการเงินอิเล็กทรอนิกส์ และธุรกรรมอื่นที่มีการพิสูจน์ตัวตนในลักษณะเดียวกัน เช่น การสมัครใช้บริการสินเชื่อ ได้ในวงกว้าง

ทั้งนี้ ผู้ให้บริการทางการเงินที่ประยุกต์ใช้เทคโนโลยีชีวมิติและผ่านการทดสอบภายใต้ regulatory sandbox แล้ว ต้องรายงานข้อมูลการใช้เทคโนโลยีชีวมิติแก่ ธปท. อย่างต่อเนื่อง ตามรายละเอียดและช่วงเวลาที่กำหนด ตามแบบรายงานที่แนบ จนกว่า ธปท. จะกำหนดเป็นอย่างอื่น

4. การประยุกต์ใช้เทคโนโลยีชีวมิติเพื่อเปรียบเทียบภาพใบหน้ากับธุรกรรมอื่น เช่น ธุรกรรมการโอนเงิน ธุรกรรมการชำระเงิน ซึ่งมีความเสี่ยง (risk profile) ที่แตกต่างไปจากการเปิดบัญชีเงินฝากหรือการเปิดใช้บริการเงินอิเล็กทรอนิกส์ หรือกับรูปแบบการให้บริการในลักษณะอื่นนอกเหนือจากข้อ 2. และ 3. ให้ผู้ให้บริการทางการเงินหารือ ธปท. ก่อนดำเนินการ

5. การประยุกต์ใช้เทคโนโลยีชีวมิติประเภทอื่นที่นอกเหนือจากการใช้เทคโนโลยีชีวมิติเพื่อเปรียบเทียบภาพใบหน้าให้หารือ ธปท. ก่อนดำเนินการ

ทั้งนี้ ท่านสามารถดาวน์โหลดแนวปฏิบัติฉบับนี้ได้ทางเว็บไซต์ของ ธปท. ได้ที่ https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2563/ThaiPDF/25630177.pdf

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวสิริธิดา พนมวัน ณ อยุธยา)
ผู้ช่วยผู้ว่าการ สายนโยบายระบบการชำระเงิน
และเทคโนโลยีทางการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน
2. แบบรายงานข้อมูลการใช้เทคโนโลยีชีวมิติ

ฝ่ายเทคโนโลยีทางการเงิน
โทรศัพท์ 0 2283 6924, 0 2283 6892
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5827

หมายเหตุ [ ] ธนาคารแห่งประเทศไทยจะจัดให้มีการประชุมชี้แจงในวันที่ ..... ณ .....
[x] ไม่มีการจัดประชุมชี้แจง

แนวปฏิบัติ

การใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

22 กรกฎาคม 2563

ธนาคารแห่งประเทศไทย

จัดทำโดย
ฝ่ายเทคโนโลยีทางการเงิน
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
ธนาคารแห่งประเทศไทย
โทรศัพท์ 0 2283 6892
0 2283 6816
e-mail: FinTechDept@bot.or.th

สารบัญ

หัวข้อ **หน้า**

1. เหตุผลในการออกแนวปฏิบัติ 3

2. ขอบเขตการใช้ 4

3. คำจำกัดความ 4

4. ภาพรวมการใช้เทคโนโลยีชีวมิติ 4

4.1 หลักการทำงานของเทคโนโลยีชีวมิติ 4

4.2 ประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ 6

5. หลักการที่พึงปฏิบัติสำหรับผู้ให้บริการทางการเงิน 6

หลักการที่ 1 กรอบนโยบายและการกำกับดูแลการใช้เทคโนโลยีชีวมิติ 7

หลักการที่ 2 การรวบรวมข้อมูลชีวมิติของผู้ใช้บริการ 7

หลักการที่ 3 การประมวลผลข้อมูลชีวมิติของผู้ใช้บริการ 8

หลักการที่ 4 การรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการ 10

หลักการที่ 5 การคุ้มครองผู้ใช้บริการ 12

หลักการที่ 6 การควบคุมความเสี่ยงด้านปฏิบัติการ 13

ภาคผนวก ก ข้อกำหนดเกี่ยวกับมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ 15

แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน (Guideline for Application of Biometric Technology in Financial Services)

1. เหตุผลในการออกแนวปฏิบัติ

เทคโนโลยีชีวมิติ (Biometric technology) เป็นเทคโนโลยีที่ใช้ในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรมของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์หรือยืนยันตัวตนบุคคล ซึ่งเทคโนโลยีชีวมิติในปัจจุบันมีพัฒนาการที่ก้าวหน้าขึ้นเป็นอย่างมาก ทั้งด้านความแม่นยำในการระบุตัวตนบุคคลและความสะดวกในการใช้งาน และได้ถูกนำมาใช้เพิ่มประสิทธิภาพการให้บริการในภาคการเงินมากขึ้น โดยเฉพาะในการระบุ พิสูจน์ และยืนยันตัวตนผู้ใช้บริการ เช่น การรู้จักผู้ใช้บริการ (Know Your Customer : KYC) สำหรับการเปิดบัญชีหรือสมัครใช้บริการต่าง ๆ เพื่อลดโอกาสการเกิดทุจริตจากการปลอมแปลงตัวบุคคลที่เปิดบัญชีหรือทำธุรกรรมทางการเงิน และเพิ่มช่องทางการให้บริการทางออนไลน์ที่ช่วยให้ผู้ใช้บริการสะดวกขึ้นโดยสามารถรู้จักผู้ใช้บริการผ่านช่องทางอิเล็กทรอนิกส์ (e-KYC) ได้อย่างน่าเชื่อถือ รวมถึงการยืนยันตัวตนสำหรับการทำธุรกรรมอื่น ๆ เพื่อเพิ่มความสะดวกแก่ผู้ใช้บริการ

อย่างไรก็ตาม การนำเทคโนโลยีชีวมิติมาใช้กับบริการทางการเงินเป็นเรื่องเกี่ยวข้องกับการใช้อัตลักษณ์ทางกายภาพหรือพฤติกรรมของบุคคลซึ่งถือเป็นข้อมูลส่วนบุคคลที่สำคัญ หากมีการบริหารจัดการที่ไม่เหมาะสมอาจส่งผลกระทบต่อความเป็นส่วนตัวของบุคคล และความเชื่อมั่นต่อระบบสถาบันการเงินในภาพรวม จึงจำเป็นต้องให้ความสำคัญในหลายมิติ ทั้งความสามารถของเทคโนโลยีในการระบุ พิสูจน์ และยืนยันตัวตน การดูแลรักษาความปลอดภัยข้อมูลส่วนบุคคล รวมทั้งการคุ้มครองและให้ความรู้แก่ผู้ใช้บริการ

ที่ผ่านมา ผู้ให้บริการทางการเงินได้เข้าร่วมทดสอบการนำเทคโนโลยีชีวมิติมาประยุกต์ใช้ในการให้บริการทางการเงินในวงจำกัด ภายใต้แนวทางการเข้าร่วมทดสอบและพัฒนานวัตกรรมที่นำเทคโนโลยีใหม่มาสนับสนุนการให้บริการทางการเงิน (Regulatory sandbox) ของธนาคารแห่งประเทศไทย (ธปท.) โดยใช้เทคโนโลยีชีวมิติเพื่อยกระดับความปลอดภัยในการพิสูจน์ตัวตนของผู้ใช้บริการสำหรับการเปิดบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ (e-Money) โดยใช้การเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้ใช้บริการกับแหล่งข้อมูลที่เชื่อถือได้ (Trusted source) เช่น ภาพจากบัตรประจำตัวประชาชน หรือหนังสือเดินทาง และ ธปท. มีการประเมินผลการทดสอบและมีกระบวนการดูแลความเสี่ยงอย่างใกล้ชิด เพื่อให้ผู้ให้บริการทางการเงินมีการดูแลความเสี่ยงที่เกี่ยวข้อง และมีแนวทางคุ้มครองผู้ใช้บริการที่เหมาะสม

ธปท. สนับสนุนการนำเทคโนโลยีมาใช้ในการพัฒนานวัตกรรมทางการเงินที่เป็นประโยชน์ต่อภาคการเงินของประเทศโดยต้องมีการบริหารจัดการความเสี่ยงจากเทคโนโลยีที่เหมาะสมควบคู่ไปด้วย จึงได้ออกแนวปฏิบัตินี้เพื่อเป็นมาตรฐานขั้นต่ำให้ผู้ให้บริการทางการเงินใช้อ้างอิงในการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินอย่างปลอดภัย น่าเชื่อถือ เพื่อให้มั่นใจว่าผู้ให้บริการทางการเงินมีนโยบายและการบริหารจัดการในการนำเทคโนโลยีชีวมิติมาใช้ด้วยกระบวนการที่เหมาะสม มั่นคงปลอดภัย เช่น การกำหนดแนวนโยบาย กระบวนการ และ การปฏิบัติในการนำเทคโนโลยีชีวมิติมาใช้อย่างปลอดภัย น่าเชื่อถือ ตลอดทั้งวงจรชีวิต (Life cycle) ของข้อมูลชีวมิติ ตั้งแต่การรวบรวมข้อมูล การเก็บข้อมูล การประมวลผลเพื่อเปรียบเทียบและตัดสินใจ และการทำลาย และสอดคล้องกับมาตรฐานสากลที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ เช่น มาตรฐาน International Organization for Standardization (ISO) National Institute of Standards and Technology (NIST) Information Systems Audit and Control Association (ISACA) และ FIDO Biometric Requirements ซึ่งจะเป็นประโยชน์ต่อการเข้าถึงบริการทางการเงินของประชาชน การรักษาเสถียรภาพของระบบสถาบันการเงิน และความเชื่อมั่นของประชาชนต่อบริการของผู้ให้บริการทางการเงิน ทั้งนี้ ผู้ให้บริการทางการเงินต้องปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information technology risk) และแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (Cyber hygiene)

2. ขอบเขตการใช้

แนวปฏิบัติฉบับนี้ มีวัตถุประสงค์เพื่อให้ผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของ ธปท. ได้แก่ สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินที่อยู่ภายใต้การกำกับของธนาคารแห่งประเทศไทย และผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงิน ที่มีการประยุกต์ใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงินนำไปปฏิบัติ

3. คำจำกัดความ

ในแนวปฏิบัติฉบับนี้

เทคโนโลยีชีวมิติ (Biometric technology) หมายถึง เทคโนโลยีที่ใช้ในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรม ของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนบุคคล

ข้อมูลชีวมิติ (Biometric data)[1] หมายถึง ข้อมูลอัตลักษณ์ของบุคคลหนึ่ง ๆ ที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีชีวมิติในการจำแนกอัตลักษณ์ทางกายภาพของบุคคล เช่น ใบหน้า ลายนิ้วมือ หรืออัตลักษณ์ทางพฤติกรรมของบุคคล เช่น การพูด การเขียน เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนของบุคคลนั้น

ข้อมูลอ้างอิงชีวมิติ (Biometric reference) หมายถึง ข้อมูลชีวมิติที่ถูกจัดเก็บไว้เป็นข้อมูลอ้างอิงเพื่อใช้เปรียบเทียบกับข้อมูลชีวมิติของบุคคล ทั้งนี้ ให้หมายความรวมถึงข้อมูลชีวมิติตั้งต้น หรือเทมเพลตชีวมิติที่มีลักษณะดังกล่าวด้วย

ข้อมูลชีวมิติตั้งต้น (Biometric sample) หมายถึง ข้อมูลชีวมิติที่เกิดจากการรวบรวมอัตลักษณ์ของบุคคลและแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ โดยข้อมูลดังกล่าวยังไม่ถูกประมวลให้เป็นเทมเพลตชีวมิติ ตัวอย่างเช่น ภาพใบหน้าที่ถูกถ่ายเพื่อนำไปใช้กับเทคโนโลยีการเปรียบเทียบใบหน้า

เทมเพลตชีวมิติ (Biometric template) หมายถึง ข้อมูลชีวมิติที่เป็นผลลัพธ์จากการประมวลข้อมูลชีวมิติตั้งต้นด้วยวิธีการทางอิเล็กทรอนิกส์ ให้อยู่ในรูปแบบที่สามารถนำไปใช้เพื่อเปรียบเทียบข้อมูลชีวมิติของบุคคล และไม่สามารถเปลี่ยนกลับเป็นข้อมูลชีวมิติตั้งต้นได้ เช่น พิกัดตำแหน่งของจุดสังเกตสำคัญต่าง ๆ บนใบหน้า

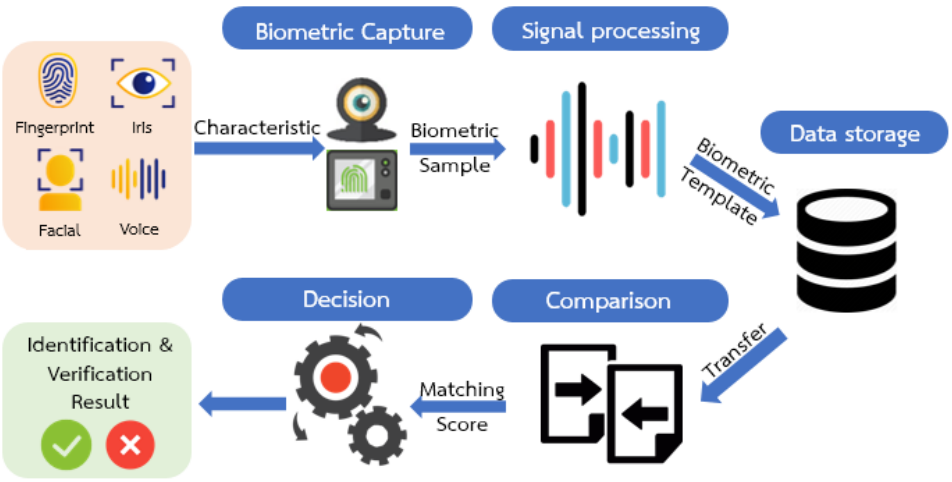
4. ภาพรวมการใช้เทคโนโลยีชีวมิติ

เทคโนโลยีชีวมิติ มีหลักการทำงาน และประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้อง ดังนี้

4.1 หลักการทำงานของเทคโนโลยีชีวมิติ

หลักการทำงานของเทคโนโลยีชีวมิติประกอบด้วย 5 ขั้นตอน คือ

[1] ข้อมูลชีวมิติ ตามแนวปฏิบัติฯ ฉบับนี้ คือข้อมูลชีวภาพตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล



(1) การรวบรวมข้อมูลชีวมิติ (Capture) เป็นขั้นตอนการรวบรวมอัตลักษณ์ของบุคคลด้วยอุปกรณ์รับข้อมูล (Sensor) ต่าง ๆ และแปลงให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ เพื่อให้ได้มาซึ่งข้อมูลชีวมิติตั้งต้น เช่น การรวบรวมภาพใบหน้าด้วยกล้อง การรวบรวมภาพลายนิ้วมือด้วยอุปกรณ์อ่านลายนิ้วมือ

(2) การประมวลอัตลักษณ์ (Signal processing) เป็นขั้นตอนการประมวลข้อมูลชีวมิติตั้งต้นให้เป็นเทมเพลตชีวมิติ ด้วยวิธีการทางอิเล็กทรอนิกส์ทำให้ไม่สามารถแปลงเทมเพลตชีวมิติให้กลับเป็นข้อมูลชีวมิติตั้งต้นได้ เช่น การประมวลผลภาพใบหน้าจากระยะห่างระหว่างจุดสังเกตสำคัญจำนวนมาก เช่น ดวงตา หางคิ้ว ความกว้างริมฝีปาก จุดสังเกตบนลายนิ้วมือ (Minutiae)

(3) การเก็บข้อมูล (Data storage) เป็นขั้นตอนการจัดเก็บข้อมูลอ้างอิงชีวมิติไว้ในระบบจัดเก็บข้อมูล ซึ่งมีการเชื่อมโยงข้อมูลอ้างอิงชีวมิติกับข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการทางการเงิน (เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน ที่อยู่) เพื่อใช้ในการเปรียบเทียบอัตลักษณ์ของบุคคลนั้น

(4) การเปรียบเทียบอัตลักษณ์ (Comparison) เป็นขั้นตอนการเปรียบเทียบระหว่างข้อมูลชีวมิติที่ต้องการระบุ พิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการ กับข้อมูลอ้างอิงชีวมิติที่เก็บไว้ในระบบจัดเก็บข้อมูลภายในองค์กรหรือแหล่งข้อมูลที่เชื่อถือได้ โดยแสดงผลการเปรียบเทียบเป็นระดับความเชื่อมั่นการเป็นบุคคลเดียวกัน ซึ่งมีการใช้งานหลักใน 2 ลักษณะ ได้แก่

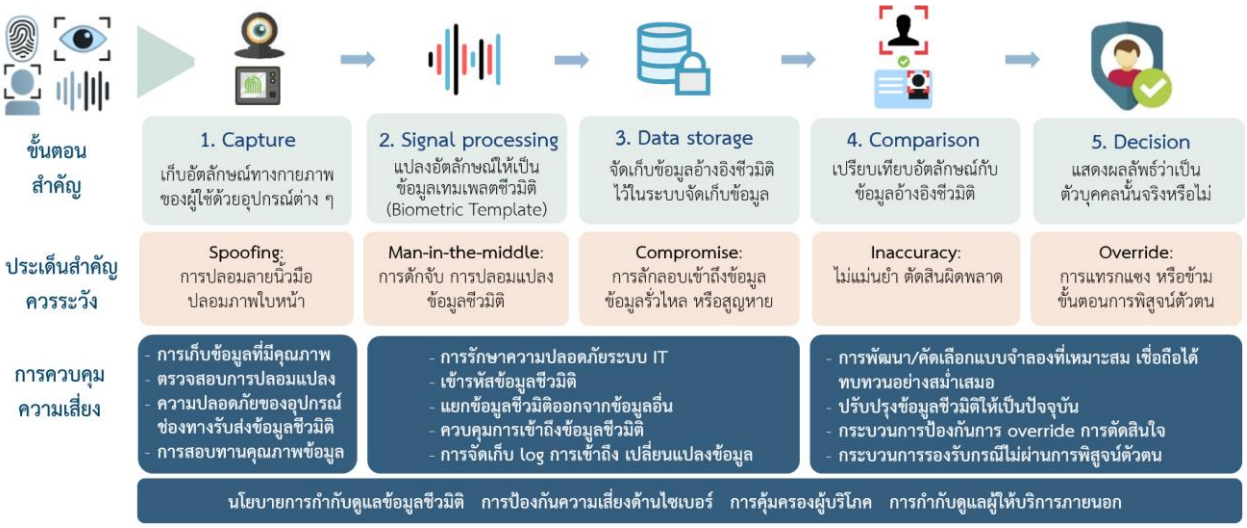
- การระบุตัวตน (Identification) คือ การนำข้อมูลชีวมิติของบุคคลมาเปรียบเทียบตัวบุคคลกับข้อมูลอ้างอิงชีวมิติที่บุคคลนั้นได้ลงทะเบียนไว้ และบันทึกอยู่ในระบบจัดเก็บแล้ว เพื่อระบุว่าเป็นบุคคลที่มีข้อมูลอยู่ในระบบจัดเก็บข้อมูลหรือไม่ เช่น การใช้ภาพใบหน้าหรือลายนิ้วมือ เพื่อค้นหาหรือระบุตัวตนของบุคคลหนึ่งที่มีข้อมูลอ้างอิงชีวมิติบันทึกไว้ในระบบจัดเก็บข้อมูลแล้ว

- การพิสูจน์ตัวตนและยืนยันตัวตน (Verification and authentication) คือ การนำข้อมูลชีวมิติของบุคคลมาเปรียบเทียบตัวบุคคลกับแหล่งข้อมูลที่เชื่อถือได้ เพื่อพิสูจน์และยืนยันว่าเป็นบุคคลนั้นจริงตามที่อ้างถึงหรือไม่ เช่น กระบวนการรู้จักผู้ใช้บริการในการเปิดบัญชีเงินฝากด้วยการเปรียบเทียบข้อมูลชีวมิติที่ได้จากการถ่ายภาพบุคคลกับข้อมูลที่บันทึกในบัตรประจำตัวประชาชน

(5) การตัดสินใจ (Decision) เป็นขั้นตอนแสดงผลลัพธ์จากการเปรียบเทียบอัตลักษณ์ของบุคคล โดยเปรียบเทียบค่าคะแนนความเชื่อมั่นที่ยอมรับได้ (Threshold) กับค่าคะแนนความเชื่อมั่นจากการเปรียบเทียบอัตลักษณ์ของบุคคล เพื่อตัดสินใจว่าเป็นบุคคลนั้นจริงหรือไม่

4.2 ประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ

เทคโนโลยีชีวมิติเกี่ยวข้องกับการใช้ข้อมูลชีวมิติของบุคคลในการระบุ พิสูจน์ หรือยืนยันตัวตน ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความสำคัญ จึงจำเป็นต้องมีการควบคุมดูแลในทุกขั้นตอนการทำงานที่เกี่ยวข้องอย่างรัดกุม ปลอดภัย โดยมีประเด็นสำคัญที่ควรพิจารณาและระมัดระวัง เพื่อป้องกันความเสี่ยงในการใช้เทคโนโลยีชีวมิติ สรุปตามแผนภาพ และคำอธิบายได้ ดังนี้



(1) การปลอมแปลงอัตลักษณ์ (Spoofing) คือ การสร้างหรือปรับแต่งลักษณะทางกายภาพและลักษณะทางพฤติกรรม เพื่อเลียนแบบอัตลักษณ์ของบุคคลอื่นด้วยวิธีต่าง ๆ เช่น การใช้วัสดุเทียมเพื่อเลียนแบบลายนิ้วมือ การใช้หน้ากากเพื่อหลอกอุปกรณ์รับข้อมูล และการใช้ภาพถ่ายหรือภาพเคลื่อนไหวที่บันทึกไว้แทนการถ่ายภาพหรือการเคลื่อนไหวจริงของบุคคล

(2) การดักจับข้อมูล (Man-in-the-middle) คือ การลักลอบคัดลอกหรือแก้ไขข้อมูลชีวมิติที่อยู่ระหว่างขั้นตอนการรับส่งข้อมูลระหว่างกันภายในระบบ เช่น การติดตั้งอุปกรณ์ดักจับข้อมูลชีวมิติในโครงข่าย

(3)การลักลอบเข้าถึงข้อมูล (Compromise) คือ การพยายามลักลอบเจาะระบบจัดเก็บข้อมูลอ้างอิงชีวมิติ เพื่อคัดลอก แก้ไข หรือทำลายข้อมูลอ้างอิงชีวมิติ

(4) การตัดสินผิดพลาด (Inaccuracy) คือ การที่ระบบระบุ พิสูจน์ หรือยืนยันตัวตนบุคคลผิดพลาดจากระดับที่กำหนด โดยอาจเกิดจากกระบวนการเปรียบเทียบอัตลักษณ์ที่ไม่แม่นยำหรือกระบวนการเรียนรู้ของระบบ (Model training) ยังไม่เพียงพอ

(5) การแทรกแซงการทำงานของระบบ (Override) คือ การพยายามแก้ไขหรือข้ามขั้นตอนการตัดสินใจของระบบการเปรียบเทียบอัตลักษณ์ เช่น การแก้ไขค่าคะแนนความเชื่อมั่นที่ยอมรับได้ให้อยู่ในระดับต่ำลง (Threshold manipulation) การปรับเปลี่ยนกระบวนการตัดสินใจโดยข้ามหรือแทรกแซงขั้นตอนประมวลผลของระบบจริง

5. หลักการที่พึงปฏิบัติสำหรับผู้ให้บริการทางการเงิน

หลักการพึงปฏิบัติที่สำคัญในการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงินมี 6 ข้อ ซึ่งผู้ให้บริการทางการเงินต้องถือปฏิบัติเป็นมาตรฐานขั้นต่ำในการให้บริการทางการเงิน โดยมีผลลัพธ์ที่คาดหวังและแนวทางที่พึงปฏิบัติ ดังนี้

หลักการที่ 1 กรอบนโยบายและการกำกับดูแลการใช้เทคโนโลยีชีวมิติ

ผลลัพธ์ที่คาดหวัง (Intended outcome) : ผู้ให้บริการทางการเงินมีความตระหนักถึงประโยชน์และความเสี่ยงในการใช้เทคโนโลยีชีวมิติ มีกรอบนโยบายที่ชัดเจนและมีกระบวนการกำกับดูแลการใช้เทคโนโลยีชีวมิติที่รัดกุมเพื่อให้ผู้ปฏิบัติงานใช้เทคโนโลยีชีวมิติและข้อมูลชีวมิติได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย สอดคล้องกับลักษณะของเทคโนโลยีชีวมิติและรูปแบบการให้บริการ

แนวทางที่พึงปฏิบัติ

(1) กำหนดให้มีกลไกการกำกับดูแลการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินที่ชัดเจน เพื่อให้มั่นใจว่ามีการคำนึงถึงการจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ ทั้งนี้ อาจใช้โครงสร้างการกำกับดูแลที่มีอยู่ในปัจจุบันหรือที่จัดตั้งขึ้นใหม่เป็นการเฉพาะ โดยโครงสร้างการกำกับดูแลดังกล่าวต้องครอบคลุมการดำเนินงานด้านต่าง ๆ ที่สำคัญ เช่น การวิเคราะห์ความเสี่ยงของเทคโนโลยีชีวมิติ ผลิตภัณฑ์ที่มีการนำเทคโนโลยีชีวมิติมาใช้ และผู้ให้บริการเทคโนโลยีที่เกี่ยวข้อง การกำหนดมาตรการบริหารจัดการความเสี่ยง มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information technology risk) และแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (Cyber hygiene)

(2) กำหนดหรือปรับปรุงนโยบายต่าง ๆ ภายในองค์กรสำหรับการกำกับดูแลข้อมูลชีวมิติ เช่น นโยบายการดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) นโยบายการกำกับดูแลข้อมูล (Data governance policy) นโยบายการจัดชั้นความลับ (Data classification policy) โดยนโยบายดังกล่าวควรมีเนื้อหาครอบคลุมวงจรชีวิตของการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงินอย่างชัดเจน ตั้งแต่การรวบรวมข้อมูล การเก็บข้อมูล การประมวลผลเพื่อเปรียบเทียบและตัดสินใจ และการทำลาย เพื่อให้ผู้ปฏิบัติงานมีความเข้าใจและสามารถนำไปปฏิบัติได้

(3) ประเมินการนำเทคโนโลยีชีวมิติมาให้บริการอย่างรอบด้านก่อนนำมาใช้ในการให้บริการ ทั้งการประเมินประโยชน์ ความเหมาะสมกับรูปแบบการให้บริการ ผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล[2] ความเสี่ยงของเทคโนโลยีชีวมิติ และแนวทางการจัดการความเสี่ยงด้านต่าง ๆ ที่สำคัญ ได้แก่ ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านกฎหมายและการปฏิบัติตามหลักเกณฑ์การกำกับดูแลที่เกี่ยวข้อง

หลักการที่ 2 การรวบรวมข้อมูลชีวมิติของผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีกระบวนการได้มาซึ่งข้อมูลชีวมิติของผู้ใช้บริการที่เหมาะสม มีการดูแลข้อมูลชีวมิติให้มีคุณภาพดีเพียงพอสำหรับการระบุ พิสูจน์ หรือยืนยันตัวตนเพื่อให้บริการทางการเงิน รวมถึงมีการสร้างความเข้าใจกับผู้ใช้บริการเพื่อสร้างความเชื่อมั่นในการนำเทคโนโลยีชีวมิติมาให้บริการ

แนวทางที่พึงปฏิบัติ

(1) กำหนดกระบวนการหรือมาตรฐานการได้มาซึ่งข้อมูลชีวมิติที่มีคุณภาพและครบถ้วนเพียงพอต่อการประมวลผลเพื่อ ระบุ พิสูจน์ หรือยืนยันตัวตนของผู้ใช้บริการอย่างถูกต้องแม่นยำ ซึ่งครอบคลุมทั้งการกำหนดแนวปฏิบัติสำหรับผู้ปฏิบัติงานที่รวบรวมข้อมูล และการให้คำแนะนำผู้ใช้บริการกรณีที่ผู้ใช้บริการดำเนินการในการให้ข้อมูลชีวมิติเอง เช่น การถ่ายภาพตนเองด้วยโทรศัพท์เคลื่อนที่ การทำรายการที่เครื่อง Kiosk เพื่อให้

[2] การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data protection impact assessment) สามารถอ้างอิงได้จากแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

มั่นใจว่าข้อมูลชีวมิติที่รวบรวมมีคุณภาพดีเพียงพอในการนำไปประมวลผลต่อไป เช่น การตรวจสอบสภาพแวดล้อมให้มีแสงสว่างเพียงพอต่อการถ่ายภาพ การให้คำแนะนำผู้ใช้บริการไม่ให้มีการสวมหมวกหรือแว่นตาดำก่อนการถ่ายภาพใบหน้า การตรวจสอบคุณภาพของภาพถ่ายก่อนบันทึกเข้าระบบ และขั้นตอนรองรับกรณีที่มีข้อจำกัดในการใช้ข้อมูลชีวมิติ เช่น ภาพในบัตรประจำตัวประชาชนไม่สามารถใช้งานได้ ลายนิ้วมือเลือนราง รวมถึงอาจใช้เทคโนโลยีการประเมินคุณภาพของภาพ เช่น Image quality assessment เข้ามาช่วยในการวิเคราะห์ประเมินคุณภาพของข้อมูลชีวมิติ

ทั้งนี้ กระบวนการและแนวทางการควบคุมคุณภาพของการรวบรวมข้อมูลชีวมิติอาจแตกต่างกันตามรูปแบบและช่องทางการให้บริการ อย่างไรก็ดี กรณีที่มีการใช้ภาพถ่ายใบหน้า ผู้ให้บริการทางการเงินควรพิจารณารายละเอียดในข้อกำหนดเกี่ยวกับมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติตามภาคผนวก ก ซึ่งสอดคล้องกับมาตรฐาน ISO 19794-5 Biometric data interchange formats -- Part 5 Face image data

(2) ชี้แจงผู้ใช้บริการเกี่ยวกับวัตถุประสงค์ของการรวบรวมข้อมูลชีวมิติอย่างชัดเจน ก่อนหรือในขณะที่จะเริ่มกระบวนการรวบรวมข้อมูลชีวมิติ พร้อมทั้งชี้แจงเกี่ยวกับประโยชน์จากการใช้เทคโนโลยีชีวมิติ สิทธิที่ผู้ใช้บริการพึงมีในการให้ข้อมูลชีวมิติ และผลกระทบที่อาจเกิดจากการที่ผู้ใช้บริการไม่ให้ข้อมูลดังกล่าว โดยคำนึงถึงการปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(3) กำหนดกลไกการตรวจสอบการปลอมแปลงอัตลักษณ์ เพื่อป้องกันการสวมรอยเป็นบุคคลอื่นในขั้นตอนการรวบรวมข้อมูลชีวมิติ ทั้งกรณีที่ผู้ให้บริการทางการเงินพบเห็นผู้ใช้บริการต่อหน้า (Face-to-face) และไม่พบเห็นผู้ใช้บริการต่อหน้า (Non face-to-face) เช่น มีการพิสูจน์ หรือยืนยันตัวตนกับแหล่งข้อมูลที่เชื่อถือได้ อย่างบัตรประจำตัวประชาชนหรือหนังสือเดินทาง มีกระบวนการหรือเทคโนโลยีตรวจจับการปลอมแปลงชีวมิติ (Presentation attack detection) เช่น Liveness detection หรือมีกระบวนการอื่นเพิ่มเติมที่รัดกุมเพียงพอ

(4) กำหนดแนวทางและกระบวนการควบคุมภายใน และมีการสอบทานความถูกต้องของกระบวนการได้มาซึ่งข้อมูลชีวมิติจากผู้ใช้บริการอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีการปฏิบัติเป็นไปตามนโยบาย แนวปฏิบัติและกระบวนการที่กำหนดไว้

(5) กำหนดแนวทางการดูแลอุปกรณ์ที่ใช้รวบรวมข้อมูลชีวมิติที่นำมาให้บริการ เช่น อุปกรณ์ถ่ายภาพและระบบงานที่สาขาหรือจุดรวบรวมข้อมูลชีวมิติ เครื่องอ่านลายนิ้วมือที่ตู้ Kiosk รวมถึงช่องทางการรับส่งข้อมูลชีวมิติของผู้ใช้บริการ ให้อยู่ในสภาพที่พร้อมให้บริการเพื่อให้สามารถรวบรวมข้อมูลได้อย่างมีคุณภาพ มีความปลอดภัย ไม่มีการเก็บหรือคงค้างข้อมูลชีวมิติอยู่ในอุปกรณ์หรือระบบที่ใช้ในการรวบรวมข้อมูลชีวมิติของผู้ให้บริการทางการเงิน ซึ่งรวมถึงกรณีที่มีการรวบรวมข้อมูลชีวมิติผ่านช่องทางของผู้ให้บริการภายนอก (3rd party service provider)

หลักการที่ 3 การประมวลผลข้อมูลชีวมิติของผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการประมวลผลอัตลักษณ์ การเปรียบเทียบอัตลักษณ์ และการตัดสินใจที่ถูกต้องแม่นยำอยู่ในระดับที่สูงเพียงพอต่อการให้บริการทางการเงิน รวมถึงสามารถป้องกันการปลอมแปลงอัตลักษณ์ เพื่อให้บริการทางการเงินมีความปลอดภัยและความน่าเชื่อถือต่อผู้ใช้บริการ

แนวทางที่พึงปฏิบัติ

(1) กำหนดแนวทางการพัฒนาหรือคัดเลือกเทคโนโลยีในการเปรียบเทียบข้อมูลชีวมิติอย่างเหมาะสม โดยคำนึงถึงความแม่นยำในการเปรียบเทียบอัตลักษณ์ที่เหมาะสมกับ รูปแบบการให้บริการ ประเภทและระดับความเสี่ยงของธุรกรรม และเทียบเคียงได้กับมาตรฐานสากล[3] รวมถึงมีความสามารถในการตรวจจับการปลอมแปลงชีวมิติ[4] เช่น การป้องกันการใช้ภาพใบหน้าหรือลายนิ้วมือปลอมแทนอัตลักษณ์จริง

ในการพัฒนาแบบจำลองหรือคัดเลือกแบบจำลองจากผู้ให้บริการภายนอก ควรคำนึงถึงการทดสอบด้วยกลุ่มตัวอย่าง (Test sample) ที่มีคุณภาพ มีปริมาณ (Sample size) และความหลากหลายมากเพียงพอ เหมาะสมกับรูปแบบของการให้บริการ[5] ทั้งนี้ แบบจำลองควรผ่านการประเมินความแม่นยำเทียบกับมาตรฐานสากล โดยองค์กรกลางหรือผู้เชี่ยวชาญที่มีความน่าเชื่อถือ ด้วยวิธีการทดสอบแบบจำลองที่สอดคล้องตามมาตรฐานสากล[6] รวมถึงมีการสอบทานและยกระดับความแม่นยำของแบบจำลองอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีความแม่นยำตามที่ผู้ให้บริการทางการเงินกำหนด

(2) มีกระบวนการตรวจสอบว่าข้อมูลและเอกสารที่ใช้เพื่อระบุ พิสูจน์ หรือยืนยันตัวตนเชื่อถือได้เป็นปัจจุบัน เช่น มีกลไกตรวจสอบความแท้จริงและเป็นปัจจุบันของบัตรประจำตัวประชาชนหรือหนังสือเดินทางที่ใช้เป็นแหล่งข้อมูลที่เชื่อถือได้ในการเปรียบเทียบอัตลักษณ์ และมีกลไกการรวบรวมข้อมูลชีวมิติที่เป็นปัจจุบันของผู้ใช้บริการ เช่น กำหนดระยะเวลาหรือเงื่อนไขในการปรับปรุงข้อมูลภาพถ่ายผู้ใช้บริการที่เหมาะสมกับลักษณะของบริการหรือธุรกรรม หรือสอดคล้องตามหลักเกณฑ์ที่เกี่ยวข้อง

(3) กำหนดกลไกการตรวจจับและป้องกันการปลอมแปลงข้อมูลชีวมิติในขั้นตอนการเปรียบเทียบอัตลักษณ์ หรือความพยายามในการข้ามหรือแทรกแซง ขั้นตอนการเปรียบเทียบอัตลักษณ์เพื่อพิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการ เช่น จำกัดจำนวนครั้งที่ผู้ใช้บริการสามารถพิสูจน์ หรือยืนยันตัวตนด้วยข้อมูลชีวมิติ

---

[3] ค่าความแม่นยำในการเปรียบเทียบอัตลักษณ์อ้างอิงตามกระบวนการทดสอบมาตรฐานสากล เช่น การพิสูจน์ตัวตนด้วยภาพใบหน้าเทียบกับแหล่งข้อมูลที่เชื่อถือได้ ควรมีค่าอัตราส่วนการยอมรับที่ผิดพลาด (False Acceptance Ratio, FAR) ไม่เกิน 0.1% ตามมาตรฐาน NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management และค่าอัตราส่วนการปฏิเสธที่ผิดพลาด (False Reject Ratio, FRR) ไม่เกิน 3% อ้างอิงตามมาตรฐาน FIDO Biometric Requirements ซึ่งกำหนดกระบวนการ วิธี และระดับความแม่นยำขั้นต่ำในการยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ

[4] การทดสอบความสามารถในการตรวจจับการปลอมแปลงชีวมิติ แบ่งตามระดับความซับซ้อนได้ดังนี้

ระดับต่ำ : ใช้อุปกรณ์ที่หาได้ทั่วไป ใช้เวลาเตรียมการน้อย ต้องการทักษะการปลอมแปลงต่ำ และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ง่ายในการปลอมแปลง (ตัวอย่างเช่น การใช้ภาพใบหน้าที่เป็นภาพนิ่งแทนใบหน้าของบุคคลจริง เช่น ภาพใบหน้าที่หาได้จาก Social media ต่าง ๆ ภาพใบหน้าจากการตัดต่อด้วยโปรแกรมตัดต่อภาพ)

ระดับปานกลาง : ใช้อุปกรณ์เฉพาะทางหรืออุปกรณ์ที่หาได้ทั่วไป ใช้เวลาในการเตรียมการปานกลาง ต้องการทักษะการปลอมแปลงระดับหนึ่ง และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ไม่ยากมากนัก ในการปลอมแปลง (ตัวอย่าง เช่น ใช้ภาพวิดีโอหรือภาพเคลื่อนไหวของบุคคลที่มีคุณภาพสูง เพื่อลอกเลียนการทำท่าทางตามกระบวนการ Liveness detection)

ระดับสูง : ใช้อุปกรณ์เฉพาะทาง ใช้เวลาในการเตรียมการมาก ต้องการทักษะการปลอมแปลงระดับสูง และอาศัยข้อมูลอัตลักษณ์ของบุคคลที่เข้าถึงได้ยาก ในการปลอมแปลง (ตัวอย่างเช่น ใช้หน้ากาก 3D mask เลียนแบบใบหน้าบุคคลจริง)

ผู้ให้บริการทางการเงินควรพิจารณาการทดสอบการปลอมแปลงโดยอ้างอิงมาตรฐานสากล เช่น NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management, ISO30701 – Biometric presentation attack detection และ FIDO Biometric Requirements

[5] ในการทดสอบเทคโนโลยีชีวมิติเพื่อการพิสูจน์และยืนยันตัวตนลูกค้าสำหรับการเปิดบัญชีเงินฝากและเงินอิเล็กทรอนิกส์ ภายใต้กรอบ Regulatory sandbox ของ ธปท. มีการกำหนดจำนวนกลุ่มตัวอย่างทดสอบขั้นต่ำอย่างน้อย 2,000 คน ขึ้นไป

[6] มาตรฐานสากลเกี่ยวกับการพัฒนาและทดสอบแบบจำลอง ได้แก่ ISO 19795 - Biometric performance testing and reporting

ได้ต่อเนื่องเพื่อป้องกันการทดลองทำซ้ำ[7] กำหนดระยะเวลาที่ระบบยอมให้ทำธุรกรรมด้วยข้อมูลชีวมิติโดยผู้ใช้บริการต้องยืนยันตัวตนใหม่หากไม่มีกิจกรรมใด ๆ เกิดขึ้น (Time-out policy)

(4) กำหนดกระบวนการรองรับกรณีที่ระบบการเปรียบเทียบอัตลักษณ์ไม่สามารถใช้งานได้ หรือกรณีที่ผู้ใช้บริการตัวจริงพิสูจน์หรือยืนยันตัวตนไม่สำเร็จ (False reject) โดยควรมีกระบวนการรองรับที่เหมาะสมกับรูปแบบการให้บริการ รวมทั้งลักษณะและความเสี่ยงของธุรกรรม เช่น การมีทางเลือกให้ผู้ใช้บริการพิสูจน์หรือยืนยันตัวตนด้วยวิธีอื่น หรือการแสดงหลักฐานอื่นเพิ่มเติมประกอบการพิสูจน์ หรือยืนยันตัวตน

(5) กำหนดแนวทางการดูแลรักษาความปลอดภัยของข้อมูลในขั้นตอนการประมวลอัตลักษณ์และขั้นตอนเปรียบเทียบอัตลักษณ์ โดยเฉพาะกรณีที่ผู้ให้บริการทางการเงินมีการใช้บริการประมวลอัตลักษณ์หรือเปรียบเทียบอัตลักษณ์ผ่านระบบของผู้ให้บริการภายนอก จะต้องไม่มีการเก็บหรือคงค้างข้อมูลชีวมิติในระบบของผู้ให้บริการภายนอก

หลักการที่ 4 การรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการดูแลรักษาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการที่เข้มงวดและรัดกุมตามมาตรฐานสากล เพื่อให้มั่นใจว่าข้อมูลของผู้ใช้บริการได้รับการปกป้องดูแลอย่างปลอดภัย

แนวทางที่พึงปฏิบัติ

(1) กำหนดนโยบายและออกแบบระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT infrastructure) ที่คำนึงถึงความปลอดภัยของข้อมูลชีวมิติและความสามารถในการขยายขนาดเพื่อรองรับปริมาณธุรกรรมที่เพิ่มขึ้นในอนาคต

(2) ไม่เก็บข้อมูลชีวมิติตั้งต้นของผู้ใช้บริการ โดยให้จัดเก็บเป็นเทมเพลตชีวมิติเพื่อใช้ในการเปรียบเทียบอัตลักษณ์ และต้องไม่สามารถแปลงย้อนกลับเป็นข้อมูลชีวมิติตั้งต้นได้ ยกเว้นกรณีภาพถ่ายใบหน้าของลูกค้า หรือกรณีที่ผู้ให้บริการทางการเงินมีความจำเป็นในการจัดเก็บข้อมูลชีวมิติตั้งต้นเพื่อปฏิบัติตามกฎหมาย นอกจากนี้ ให้ปฏิบัติตามกฎหมายที่เกี่ยวข้องด้วย เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(3) กำหนดกระบวนการจัดเก็บ รับส่ง และเชื่อมโยงข้อมูลอ้างอิงชีวมิติ ที่มีความรัดกุมปลอดภัย ได้แก่

(3.1) จัดเก็บและรับส่งข้อมูลอ้างอิงชีวมิติเพื่อให้ไม่สามารถระบุตัวตนเจ้าของข้อมูล และไม่สามารถนำไปใช้ต่อได้โดยไม่ได้รับอนุญาต เช่น การเข้ารหัสข้อมูลอ้างอิงชีวมิติสำหรับการรับส่งข้อมูล (Data-in-transit) ระหว่างขั้นตอนต่าง ๆ ตั้งแต่อุปกรณ์รับข้อมูล สายสื่อสาร จนถึงการบันทึกข้อมูลอ้างอิงชีวมิติ (Data-at-rest) มีการเข้ารหัสในระดับฟิลด์ของระบบจัดเก็บข้อมูลหรือระดับไฟล์ ด้วยมาตรฐานการเข้ารหัสข้อมูลที่มีความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น อัลกอริธึมการเข้ารหัส (Encryption algorithm) และขนาดความยาวของกุญแจเข้ารหัสข้อมูล เป็นต้น รวมถึงมีกระบวนการเก็บรักษากุญแจเข้ารหัสที่มีความรัดกุม

---

[7] สามารถอ้างอิงการกำหนดจำนวนครั้งและระยะเวลาตามมาตรฐาน NIST SP 800-63B Digital Identity Guidelines Authentication and Lifecycle Management และ ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจำกัดจำนวนครั้งของการยืนยันตัวตนด้วยชีวมิติให้ผิดพลาดอย่างต่อเนื่องได้ไม่เกิน 5 ครั้งกรณีทั่วไป หรือไม่เกิน 10 ครั้ง กรณีที่ใช้งานการตรวจจับการปลอมแปลงชีวมิติ โดยหากครบกำหนดแล้วต้องดำเนินการอย่างใดอย่างหนึ่ง ดังนี้

- หน่วงเวลาอย่างน้อย 30 วินาทีก่อนอนุญาตให้ยืนยันตัวตนครั้งถัดไป และเพิ่มการหน่วงเวลาก่อนอนุญาตให้ยืนยันตัวตนครั้งต่อไปแบบ Exponential เช่น หน่วงเวลาอย่างน้อย 30 วินาที 1 นาที 2 นาที 4 นาที 8 นาที และเพิ่มขึ้นตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด
- ระงับการยืนยันตัวตนด้วยชีวมิติและให้ผู้ใช้บริการยืนยันตัวตนด้วยวิธีอื่น

(3.2) จัดเก็บข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการแยกออกจากข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการ เช่น ชื่อ-นามสกุล หรือเลขประจำตัวประชาชน ในระดับเซิร์ฟเวอร์หรือฐานข้อมูล เพื่อป้องกันไม่ให้ข้อมูลอ้างอิงชีวมิติรั่วไหลพร้อมข้อมูลส่วนบุคคลอื่นของผู้ใช้บริการ เช่น ระบบฐานข้อมูลภาพใบหน้าแยกจากระบบฐานข้อมูลทั่วไปของผู้ใช้บริการ จัดให้มีการดูแลและการเข้าถึงทั้งสองระบบแยกจากกัน รวมถึงหากมีการเข้ารหัสข้อมูลต้องใช้กุญแจเข้ารหัส (Encryption key) ที่แตกต่างกัน

(3.3) ไม่ระบุข้อมูลอ้างอิงชีวมิติโดยอ้างอิงด้วยข้อมูลที่สามารถใช้ระบุตัวตนของผู้ใช้บริการได้โดยตรง (Indirect reference) เช่น เลขประจำตัวประชาชน และเลขประจำตัวผู้ใช้บริการที่ออกโดยผู้ให้บริการทางการเงินซึ่งถูกใช้งานเพื่ออ้างอิงตัวบุคคลของผู้ใช้บริการได้ในหลายระบบงานของผู้ให้บริการทางการเงิน เพื่อป้องกันไม่ให้สามารถระบุตัวตนของข้อมูลอ้างอิงชีวมิติได้หากเกิดเหตุการณ์โจมตีหรือข้อมูลรั่วไหล

(3.4) แบ่งขอบเขตเครือข่าย (Network zoning) และจัดวางระบบและข้อมูลอ้างอิงชีวมิติ โดยคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ไม่จัดวางระบบและข้อมูลอ้างอิงชีวมิติใน Demilitarized zone (DMZ) เพื่อป้องกันผลกระทบหรือการโจมตีจากเครือข่ายที่ไม่ปลอดภัย

(3.5) ใช้ช่องทางสื่อสารและวิธีการที่ปลอดภัยในการรับส่งข้อมูลชีวมิติระหว่างระบบงานทั้งภายนอกและภายในหน่วยงาน

(4) มีกระบวนการควบคุมการเข้าถึงข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการอย่างเข้มงวด การให้สิทธิการเข้าถึงข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการเท่าที่จำเป็นโดยผู้ปฏิบัติงานที่เกี่ยวข้องเท่านั้น และมีการสอบทานสิทธิอย่างสม่ำเสมอ รวมถึงการมีกระบวนการตรวจสอบความถูกต้องเชื่อถือได้ (Integrity check) ของข้อมูลอ้างอิงชีวมิติเพื่อป้องกันการลักลอบเปลี่ยนแปลงหรือแก้ไขข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการโดยไม่ได้รับอนุญาต

(5) มีการบริหารจัดการช่องโหว่ (Vulnerability management) ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยผู้ให้บริการทางการเงินต้องประเมินช่องโหว่ของระบบโครงสร้างพื้นฐานที่เกี่ยวข้องกับข้อมูลชีวมิติอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงผู้ให้บริการเทคโนโลยีชีวมิติ หรือเมื่อมีการแจ้งเตือนช่องโหว่ด้านความปลอดภัยที่มีผลกระทบกับระบบที่มีความเกี่ยวข้องกับข้อมูลชีวมิติเป็นวงกว้าง เป็นต้น

(6) มีการทดสอบเจาะระบบ (Penetration test) โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

(7) มีกระบวนการแก้ไขจุดอ่อนความปลอดภัยของระบบ (Patch management) ซึ่งครอบคลุมระบบงานที่รองรับการประมวลผลและจัดเก็บข้อมูลอ้างอิงชีวมิติ รวมถึงกระบวนการสนับสนุนทางด้านอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ (Hardware and software support) รองรับกรณีที่เทคโนโลยีนั้นมีจุดอ่อนหรือตรวจพบความผิดพลาด โดยผู้ให้บริการเทคโนโลยีชีวมิติจะต้องสามารถแก้ไขจุดอ่อนของเทคโนโลยีได้อย่างทันท่วงทีที่มีการแจ้งเตือน

(8) จัดเก็บบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับข้อมูลชีวมิติ โดยครอบคลุมบันทึกการเข้าถึง (Access log) บันทึกการดำเนินงาน (Activity log) บันทึกร่องรอยการทำกิจกรรมธุรกรรม (Transaction log) และบันทึกด้านการรักษาความปลอดภัย (Security event log) ด้วยวิธีการที่มีความปลอดภัยและมีความเพียงพอต่อการสอบทานย้อนหลัง การตรวจสอบในกรณีเกิดเหตุการณ์ผิดปกติ และการใช้เป็นหลักฐานทางกฎหมาย

(9) กำหนดนโยบายและการดูแลข้อมูลชีวมิติอย่างเข้มงวด ในกรณีใช้เทคโนโลยีคลาวด์คอมพิวติ้ง (Cloud computing) เพื่อการประมวลผลหรือเก็บข้อมูลอ้างอิงชีวมิติของผู้ใช้บริการ โดยมีการควบคุมการเข้าถึงข้อมูลอย่างรัดกุม มีการประเมินมาตรฐานการรักษาความปลอดภัยข้อมูลของผู้ให้บริการคลาวด์ (Cloud service provider) โดยคำนึงปัจจัยที่เกี่ยวข้อง[8] เช่น การได้รับใบรับรองมาตรฐานสากลด้านความปลอดภัยข้อมูล นโยบายการดูแลความปลอดภัยข้อมูลของผู้ให้บริการ การประเมินความเสี่ยงจากการกระจุกตัว (Concentration risk) ของระบบคลาวด์ที่จัดเก็บข้อมูลอ้างอิงชีวมิติ รวมถึงการจัดทำข้อตกลงให้ผู้ให้บริการทางการเงินสามารถเข้าตรวจสอบการจัดเก็บข้อมูลได้ และการมีกระบวนการรองรับความพร้อมใช้ของระบบและเก็บข้อมูลอ้างอิงชีวมิติเพื่อความพร้อมใช้ภายในประเทศ

(10)กำหนดให้มีการตรวจสอบกระบวนการรักษาความปลอดภัยข้อมูลชีวมิติของผู้ใช้บริการอย่างสม่ำเสมอ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือผู้ตรวจสอบภายนอก (External auditor) ซึ่งครอบคลุมกรณีที่ใช้บริการจากผู้ให้บริการภายนอก

หลักการที่ 5 การคุ้มครองผู้ใช้บริการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีแนวทางคุ้มครองผู้ใช้บริการและมีการให้ความรู้เกี่ยวกับการทำธุรกรรมด้วยเทคโนโลยีชีวมิติอย่างเพียงพอ เหมาะสม เพื่อให้ผู้ใช้บริการได้รับบริการด้วยความปลอดภัย เป็นธรรม และสอดคล้องกับกฎหมายที่เกี่ยวข้อง โดยคงไว้ซึ่งการคุ้มครองสิทธิและข้อมูลส่วนบุคคล

แนวทางที่พึงปฏิบัติ

(1) จัดให้มีกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลชีวมิติให้เป็นไปตามที่กฎหมายกำหนด เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลชีวมิติ ผู้ให้บริการทางการเงินต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ เว้นแต่เข้าข้อยกเว้นตามกฎหมาย ในกรณีที่ต้องได้รับความยินยอม ผู้ให้บริการทางการเงินจะต้องได้รับความยินยอมจากผู้ใช้บริการก่อนหรือในขณะนั้น (Opt-in consent) นอกจากนี้ การเก็บรวบรวมข้อมูลชีวมิติ ให้เก็บรวบรวมได้เฉพาะเท่าที่มีความจำเป็น โดยผู้ให้บริการทางการเงินต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมให้ผู้ใช้บริการทราบก่อนหรือในขณะที่เก็บรวบรวม เช่น เพื่อการเข้าทำสัญญา หรือเพื่อการให้บริการทางการเงินเพิ่มเติม และผู้ให้บริการทางการเงินต้องใช้ข้อมูลชีวมิติดังกล่าวตามวัตถุประสงค์ที่ผู้ใช้บริการได้ให้ความยินยอมหรือตามที่กฎหมายกำหนดเท่านั้น รวมทั้งผู้ให้บริการทางการเงินต้องแจ้งให้ผู้ใช้บริการทราบถึงรายละเอียดต่าง ๆ ตามที่กฎหมายกำหนด เช่น ประเภทของบุคคลหรือหน่วยงานที่อาจได้รับข้อมูลชีวมิติหรือข้อมูลที่เกี่ยวข้องจากผู้ให้บริการทางการเงินเพื่อประโยชน์ในการให้บริการ

(2) จัดให้มีการขอความยินยอมตามที่กฎหมายกำหนด โดยผู้ให้บริการทางการเงินต้องขอความยินยอมจากผู้ใช้บริการ โดยทำเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ และต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ไม่ก่อให้เกิดความเข้าใจผิด และต้องให้อิสระแก่ผู้ใช้บริการในการตัดสินใจให้ความยินยอมด้วยความสมัครใจ นอกจากนี้ หากจะมีการใช้ข้อมูลชีวมิติแตกต่างไปจากวัตถุประสงค์ที่ผู้ใช้บริการได้ให้ความยินยอมไว้ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงข้อกำหนดการให้บริการซึ่งส่งผลกระทบกับขอบเขตความยินยอมเดิมที่ผู้ใช้บริการได้ให้ไว้ ผู้ให้บริการทางการเงินต้องขอความยินยอมจากผู้ใช้บริการใหม่อีกครั้งก่อน โดยแสดงข้อกำหนดที่มีการเปลี่ยนแปลงให้ผู้ใช้บริการเห็นได้อย่างชัดเจน เพื่อที่ผู้ใช้บริการจะได้รับทราบข้อมูลที่เป็นปัจจุบันเกี่ยวกับการใช้งานข้อมูลชีวมิติและสิทธิของผู้ใช้บริการ

[8] ผู้ให้บริการทางการเงินสามารถอ้างอิงแนวทางการประเมินผู้ให้บริการคลาวด์ตามแนวปฏิบัติ ธปท. ว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

(3) แจ้งให้ผู้ใช้บริการทราบถึงสิทธิของผู้ใช้บริการในฐานะเจ้าของข้อมูลชีวมิติ เช่น สิทธิขอเข้าถึงข้อมูลชีวมิติ สิทธิขอเปลี่ยนแปลงข้อมูลชีวมิติให้เป็นปัจจุบันและสมบูรณ์ รวมถึงเงื่อนไขที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น ผลกระทบต่อสิทธิหรือบริการที่จะได้รับในกรณีที่ผู้ใช้บริการประสงค์จะไม่ให้เก็บรวบรวมข้อมูลชีวมิติ ทั้งนี้ต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกำหนด

(4) จัดให้มีกระบวนการคุ้มครองผู้ใช้บริการในฐานะเจ้าของข้อมูลชีวมิติ เช่น การจัดให้ผู้ใช้บริการสามารถตรวจสอบประวัติการให้ความยินยอมที่เกี่ยวข้องกับข้อมูลชีวมิติ การจัดให้ผู้ใช้บริการสามารถถอนความยินยอมได้ตามหลักเกณฑ์ที่กฎหมายกำหนด โดยจัดให้มีช่องทางรับเรื่องร้องเรียนหรือแจ้งปัญหาจากการใช้บริการที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ และมีการกำหนดระยะเวลาในการแก้ปัญหา (Service level agreement) ที่ชัดเจน รวมถึงมีแนวทางสื่อสารกับผู้ใช้บริการ และหน่วยงานกำกับดูแลที่เกี่ยวข้อง กรณีที่เกิดเหตุการณ์ที่มีผลกระทบกับข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการ รวมถึงมีมาตรการเยียวยาผู้ใช้บริการที่ได้รับผลกระทบ

(5) ให้ความรู้แก่ผู้ใช้บริการเกี่ยวกับการนำเทคโนโลยีชีวมิติมาให้บริการในภาคการเงิน เพื่อให้เข้าใจถึงประโยชน์และสิทธิของผู้ใช้บริการที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ

(6) กำหนดให้มีกระบวนการเปิดเผยข้อมูลชีวมิติตามที่กฎหมายกำหนด โดยในกรณีที่มีการส่งข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติของผู้ใช้บริการให้บุคคลที่สาม เช่น ผู้ให้บริการภายนอก ผู้ให้บริการทางการเงินต้องได้รับความยินยอมจากผู้ใช้บริการก่อนหรือในขณะนั้น หรือเป็นไปตามที่กฎหมายกำหนด และต้องดำเนินการอย่างระมัดระวัง โดยต้องแจ้งข้อมูลเกี่ยวกับเปิดเผยหรือส่งข้อมูลชีวมิตินั้นให้ผู้ใช้บริการทราบ รวมทั้งให้บุคคลที่สามที่ได้รับข้อมูลชีวมิติของผู้ใช้บริการ สามารถใช้งานข้อมูลชีวมิติได้เท่าที่ได้รับความยินยอมหรือตามที่กฎหมายกำหนดเท่านั้น

หลักการที่ 6 การควบคุมความเสี่ยงด้านปฏิบัติการ

ผลลัพธ์ที่คาดหวัง : ผู้ให้บริการทางการเงินมีการบริหารจัดการความเสี่ยงด้านปฏิบัติการที่สำคัญโดยครอบคลุมทั้งกระบวนการรองรับการให้บริการอย่างต่อเนื่อง การตรวจสอบธุรกรรมที่อาจผิดปกติ รวมถึงมีกระบวนการควบคุมต่าง ๆ ที่เกี่ยวข้องกับผู้ให้บริการภายนอก เพื่อให้มั่นใจได้ว่าผู้ใช้บริการจะได้รับบริการทางการเงินด้วยเทคโนโลยีชีวมิติที่มั่นคงปลอดภัยและเชื่อถือได้

แนวทางที่พึงปฏิบัติ

(1) มีแนวทางรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business continuity plan) สำหรับการให้บริการทางการเงินด้วยเทคโนโลยีชีวมิติ ซึ่งครอบคลุมระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและกระบวนการปฏิบัติงานหากระบบขัดข้อง นอกจากนี้ผู้ให้บริการทางการเงินควรมีแผนรับมือเหตุการณ์ฉุกเฉินด้านไซเบอร์ที่ครอบคลุมข้อมูลที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น เหตุการณ์พยายามลักลอบเข้าถึงข้อมูล เหตุการณ์ข้อมูลรั่วไหล รวมถึงมีการซักซ้อมการดำเนินการตามแผนดังกล่าวอย่างสม่ำเสมอ

(2) มีกระบวนการวิเคราะห์ ตรวจสอบธุรกรรมที่อาจผิดปกติ (Fraud monitoring) ที่เกี่ยวกับการทำธุรกรรมด้วยข้อมูลชีวมิติ เช่น การเปลี่ยนภาพใบหน้าของผู้ใช้บริการหลายครั้งภายในช่วงเวลาสั้น ๆ มีการกำหนดมาตรการพิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการเพิ่มเติม เพื่อให้สามารถพิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการได้อย่างมั่นใจมากขึ้นตามความจำเป็น เช่น การขอข้อมูลหรือเอกสารพิสูจน์ตัวตนอื่น ๆ จากแหล่งข้อมูลที่เชื่อถือได้ การส่งเรื่องให้ทีมงานเฉพาะด้านพิจารณาในเชิงลึก เป็นต้น

(3) มีการบริหารจัดการผู้ให้บริการภายนอกที่เกี่ยวข้องกับข้อมูลชีวมิติ เช่น การรวบรวมข้อมูลชีวมิติ การประมวลอัตลักษณ์และการเปรียบเทียบอัตลักษณ์ของผู้ใช้บริการผ่านช่องทางตัวแทน การเก็บข้อมูลอ้างอิงชีวมิติบนระบบคลาวด์คอมพิวติ้ง ต้องมีการวิเคราะห์ความเสี่ยงและกำหนดแนวทางป้องกันความเสี่ยงอย่างรัดกุม รวมถึงมีการทำสัญญาหรือข้อตกลงโดยระบุหน้าที่ ความรับผิดชอบ สิทธิในการตรวจสอบโดยหน่วยงานผู้กำกับดูแล และเงื่อนไขการให้บริการระหว่างกันโดยเฉพาะในเรื่องการดูแลข้อมูลชีวมิติของผู้ใช้บริการ และต้องคำนึงถึงความต่อเนื่องในการดำเนินธุรกิจรวมถึงการป้องกันความเสี่ยงที่อาจเกิดจากการยกเลิกหรือสิ้นสุดสัญญาข้อตกลง เพื่อให้ผู้ให้บริการทางการเงินสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และพร้อมรับการเปลี่ยนแปลงด้านเทคโนโลยีที่อาจเกิดขึ้นในอนาคต

ภาคผนวก ก
ข้อกำหนดเกี่ยวกับมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ

1. หลักการและเหตุผล

ธปท. จัดทำข้อกำหนดนี้ขึ้นเพื่อให้ผู้ให้บริการทางการเงินมีมาตรฐานขั้นต่ำและแนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าของผู้ใช้บริการ ในการที่จะได้รับข้อมูลที่มีคุณภาพเพียงพอต่อการนำไปประมวลผลเพื่อ ระบุ พิสูจน์ หรือยืนยันตัวตนผู้ใช้บริการได้อย่างแม่นยำ น่าเชื่อถือ สอดคล้องกับมาตรฐานสากล

2. รายละเอียดของข้อกำหนด

ส่วนที่ 1 มาตรฐานขั้นต่ำสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ[9]

การรวบรวมภาพใบหน้า ทั้งกรณีที่ผู้ให้บริการทางการเงินพบเห็นผู้ใช้บริการต่อหน้า และไม่พบเห็นผู้ใช้บริการต่อหน้า ภาพใบหน้าต้องมีคุณลักษณะอย่างน้อยดังต่อไปนี้

1.1 ความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels หรือ 1080 x 1080 pixels

1.2 การบีบอัดข้อมูลภาพถ่ายควรใช้การบีบอัดข้อมูลแบบไม่สูญเสีย (Lossless data compression) หรือในกรณีที่ใช้การบีบอัดข้อมูลแบบสูญเสียบางส่วน (Lossy data compression) ต้องตรวจสอบให้มั่นใจได้ว่าคุณภาพของภาพอยู่ในระดับที่เพียงพอต่อการใช้งาน

1.3 ภาพเป็นชนิดภาพสี

1.4 ลูกค้าต้องแสดงใบหน้าทั้งหมด ในลักษณะปกติ (ไม่ยิ้ม และปากปิด) ใบหน้าตรง และมองตรงมายังกล้อง

1.5 ภาพต้องคมชัด และอยู่ในโฟกัส

1.6 ภาพต้องแสดงส่วนของศีรษะทั้งหมดของผู้ใช้บริการโดยปราศจากสิ่งปกคลุม ยกเว้นกรณีสวมเครื่องแต่งกายของศาสนา หรือวัสดุทางการแพทย์ ทั้งนี้ ภาพต้องแสดงใบหน้าทั้งหมดของผู้ใช้บริการอย่างชัดเจน

1.7 ภาพต้องแสดงดวงตาของผู้ใช้บริการอย่างชัดเจน และไม่มีสีแดง (Red-eye)

1.8 ผู้ใช้บริการสามารถใส่แว่นสายตาขณะถ่ายภาพ หากภาพที่ถ่ายออกมาแสดงให้เห็นดวงตาอย่างชัดเจนโดยไม่มีเงาหรือแสงสะท้อนจากแว่น

1.9 ผู้ใช้บริการไม่สามารถใส่แว่นตากันแดด หรือแว่นเคลือบสีขณะถ่ายภาพ

1.10 ความยาวของใบหน้า (จากศีรษะถึงคาง) ประมาณร้อยละ 60-80 ของความสูงของภาพ

---

[9] อ้างอิงตามมาตรฐาน ISO 19794-5 Biometric data interchange formats -- Part 5 Face image data และข้อเสนอแนะมาตรฐานฯ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคารของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

1.11 ภาพต้องไม่แสดงส่วนหนึ่งส่วนใดของบุคคลหรือวัตถุอื่นบนใบหน้าของผู้ใช้บริการหรือบนฉากหลังของภาพ ในลักษณะที่อาจส่งผลกระทบต่อความสามารถในการนำไปใช้เพื่อการเปรียบเทียบข้อมูลชีวมิติอย่างมีนัยสำคัญ

1.12 ใบหน้าของผู้ใช้บริการที่ปรากฏอยู่ในภาพต้องมีความสว่างเพียงพอ

ส่วนที่ 2 แนวปฏิบัติที่ดีสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติ[10]

ผู้ให้บริการทางการเงินอาจมีกระบวนการการถ่ายภาพและมีองค์ประกอบของภาพตามคุณลักษณะดังต่อไปนี้ เพื่อให้มั่นใจว่าผู้ให้บริการทางการเงินได้รับภาพที่มีคุณภาพที่ดีสำหรับนำไปประมวลผลต่อไป

2.1 ใบหน้าไม่ควรมีการก้ม เงย หัน หรือเอียงในระดับที่อาจส่งผลกระทบต่อความสามารถในการนำไปใช้เพื่อการเปรียบเทียบข้อมูลชีวมิติอย่างมีนัยสำคัญ

2.2 ไม่ควรมีเงามืดในเบ้าตาปรากฏบนใบหน้า

2.3 ความกว้างของใบหน้า (จากหูซ้ายถึงหูขวา) ประมาณร้อยละ 60-75 ของความกว้างของภาพ

2.4 ฉากหลังของภาพควรมีสีอ่อนและไม่มีลวดลาย รวมถึงไม่ปรากฏเงาของผู้ใช้บริการบนฉากหลังเพื่อให้สามารถแยกแยะใบหน้าของผู้ใช้บริการและฉากหลังได้อย่างชัดเจน

2.5 ไม่ควรมีใบหน้าของบุคคลอื่นปรากฏอยู่ในภาพ หรือมีระบบที่มีความสามารถในการแยกภาพใบหน้าของผู้ใช้บริการจากบุคคลอื่นอย่างแม่นยำ

2.6 ควรจัดให้มีสภาพแวดล้อมที่มีแสงเพียงพอต่อการถ่ายภาพสำหรับกรณีการถ่ายภาพที่สาขาหรือจุดให้บริการ และมีคำแนะนำสภาพแวดล้อมที่เหมาะสมแก่ผู้ใช้บริการในการถ่ายภาพกรณีการถ่ายภาพด้วยตนเองผ่านโทรศัพท์เคลื่อนที่ ทั้งนี้ แสงที่ตกกระทบบนใบหน้าควรมีความสม่ำเสมอ โดยไม่มีจุดสว่าง (Hot spots) ปรากฏโดยเด่นชัดบนใบหน้า

2.7 ในขณะที่ทำการถ่ายภาพ ควรมีการแสดงกรอบ หรือเส้นช่วยนำ ในจอภาพของผู้ปฏิบัติงานหรือหน้าจอโทรศัพท์เคลื่อนที่หรือคอมพิวเตอร์ของผู้ใช้บริการ ที่จะช่วยให้สามารถปรับเปลี่ยนตำแหน่งการถ่ายภาพเพื่อให้ได้ภาพถ่ายที่มีคุณภาพตามที่กำหนดได้ง่ายขึ้น

[10] อ้างอิงตามมาตรฐาน ISO 19794-5 Biometric data interchange formats -- Part 5 Face image data และข้อเสนอแนะมาตรฐานฯ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคารของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เอกสารแนบ 2

แบบรายงานข้อมูลการใช้เทคโนโลยี Biometrics

ชื่อผู้ให้บริการ.....

สำหรับรอบสิ้นสุดวันที่.....

หัวข้อ	การรายงานข้อมูล	ความถี่	กำหนดส่ง
1. ความแม่นยำของเทคโนโลยี Biometrics	1) Accuracy rate 2) False acceptance rate 3) False rejection rate	ราย 6 เดือน หรือเมื่อมีการปรับปรุงแบบจำลอง	ภายใน 21 วันนับจากวันสิ้นงวดที่รายงาน หากวันที่ครบกำหนดส่งตรงกับวันหยุดให้ส่งข้อมูลภายในวันทำการถัดไป
2. ความพร้อมใช้ของระบบที่เกี่ยวข้องกับการใช้ Biometrics	ร้อยละ ..... (ไม่นับรวม maintenance downtime)	รายไตรมาส	
3. ปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยี Biometrics รวมถึงแนวทางแก้ปัญหา (ถ้ามี)	1) จำนวนและรายละเอียดข้อร้องเรียน 2) จำนวนและเหตุการณ์ทุจริต 3) จำนวนและข้อผิดพลาดที่พบ 4) ประเด็นอื่น ๆ ที่พบ	รายไตรมาส	

<u>หมายเหตุ</u>

1. Accuracy rate = $\frac{\text{(True Accept+True Reject)}}{\text{(True Accept+True Reject+False Accept+False Reject)}} \times 100$

2. False acceptance rate = $\frac{\text{False Accept}}{\text{False Accept+True Reject}} \times 100$

3. False rejection rate = $\frac{\text{False Reject}}{\text{False Reject+True Accept}} \times 100$

ภาคผนวก 5 มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล
เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ เกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล
สำหรับบุคคลธรรมดาที่มีสัญชาติไทย
(DIGITALIZATION: DIGITAL ID - IDENTITY PROOFING AND AUTHENTICATION) พ.ศ. ๒๕๖๔

มาตรฐานรัฐบาลดิจิทัล

DIGITAL GOVERNMENT STANDARD

มรด. ๑ - ๒ : ๒๕๖๔

DGS 1 - 2 : 2564

ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

DIGITALIZATION: DIGITAL ID - IDENTITY PROOFING AND AUTHENTICATION

เวอร์ชัน ๑.๐

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการจัดทำกระบวนการ และการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

มรด. ๑ - ๒ : ๒๕๖๔

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
อาคารบางกอกไทยทาวเวอร์ ชั้น ๑๗
เลขที่ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐
หมายเลขโทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑, ๐ ๒๖๑๒ ๖๐๑๒

ประกาศโดย
คณะกรรมการพัฒนารัฐบาลดิจิทัล
วันที่ ๑๖ กันยายน ๒๕๖๔

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

นายกรัฐมนตรี ประธานกรรมการ
มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี (นายดอน ปรมัตถ์วินัย)

กรรมการ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ปลัดสำนักนายกรัฐมนตรี
ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้อำนวยการสำนักงบประมาณ
เลขาธิการคณะกรรมการข้าราชการพลเรือน
เลขาธิการคณะกรรมการพัฒนาระบบราชการ
เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการข้อมูลข่าวสารของราชการ
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

กรรมการและเลขานุการ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะอนุกรรมการสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล

ประธานอนุกรรมการ

นายสมคิด จิรานันตรัตน์

อนุกรรมการ

ผู้แทนกระทรวงเกษตรและสหกรณ์
ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้แทนกระทรวงสาธารณสุข
ผู้แทนกรมการปกครอง
ผู้แทนกรมบัญชีกลาง
ผู้แทนกรมศุลกากร
ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา
ผู้แทนสำนักงานคณะกรรมการข้าราชการพลเรือน
ผู้แทนสำนักงานคณะกรรมการพัฒนาระบบราชการ
ผู้แทนสำนักงบประมาณ
ผู้แทนสำนักงานการตรวจเงินแผ่นดิน
ผู้แทนธนาคารแห่งประเทศไทย
ผู้ทรงคุณวุฒิด้านสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล

อนุกรรมการและเลขานุการร่วม

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

รองประธานกรรมการ

นายวิบูลย์ ภัทรพิบูล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายสุทธิศักดิ์ ตันตะโยธิน	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายพณชิต กิตติปัญญางาม	สมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปณิศา เหลืองวรเมท	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายศุภโชค จันทรประทิน	
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร	สำนักงานคณะกรรมการกฤษฎีกา
นางสาวพัชรี ไชยเรืองกิตติ	
นางสาวสุภร สุขะตุงคะ	สำนักงานการตรวจเงินแผ่นดิน
นางสาวพลอยรวี เกริกพันธ์กุล	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายทรงพล ใหม่สาลี	สำนักงานสถิติแห่งชาติ
นางกาญจนา ภู่มาลี	

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

คณะทำงาน

นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายชาลี วรกุลพิพัฒน์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
รองศาสตราจารย์เกริก ภิรมย์โสภา	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

นางสาวอัญชลี โพธิ์อ่อน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวนงลักษณ์ พลอยสุภา	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายภัทร วานิชทวีวัฒน์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาววีรวรรณ วระแสง	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและแนวทางในการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ใช้บริการที่ต้องการใช้บริการภาครัฐด้วยดิจิทัลไอดี เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยพัฒนาตามแนวมาตรฐานของ

- NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing, National Institute of Standards and Technology, US Department of Commerce [๒]
- NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management, National Institute of Standards and Technology, US Department of Commerce [๓]
- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]
- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

อีกทั้งได้มีการรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้มาตรฐานรัฐบาลดิจิทัลฉบับนี้มีความครบถ้วนสมบูรณ์ สามารถนำไปปรับใช้ในทางปฏิบัติได้

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ฉบับนี้ จัดทำขึ้นโดยคณะกรรมการจัดทำร่างร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ ร่วมกับ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ
แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐
โทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐
โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑, ๐ ๒๖๑๒ ๖๐๑๒
E-mail: contact@dga.or.th
Website: www.dga.or.th

คำนำ

การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลของภาครัฐ เป็นการวางรูปแบบร่วมกันเพื่อสร้างขั้นตอนการทำงาน พัฒนาบริการให้เป็นรูปแบบดิจิทัลแบบครบวงจร สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานได้ โดยมีการนำระบบเทคโนโลยีดิจิทัลมาใช้ในการทำงาน เป็นกลไกในการเพิ่มประสิทธิภาพในการให้บริการภาครัฐแก่ประชาชน เป็นการเพิ่มทางเลือกให้แก่ประชาชนในการขอรับบริการจากภาครัฐ ช่วยลดความผิดพลาด ยกระดับการทำงานของภาครัฐผ่านระบบดิจิทัลตั้งแต่ต้นจนจบได้อย่างสมบูรณ์ นำไปสู่การเป็นรัฐบาลดิจิทัลที่ไร้กระดาษ (paperless) ซึ่งกระบวนการหลักของการดำเนินงานทางดิจิทัลของภาครัฐเริ่มตั้งแต่การพิสูจน์และยืนยันตัวตนทางดิจิทัลไปจนถึงการจัดส่งใบอนุญาตหรือเอกสารต่าง ๆ ทางดิจิทัล

การพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นกระบวนการแรกที่สำคัญในการเข้าสู่บริการภาครัฐ ซึ่งหน่วยงานของรัฐต้องประเมินความต้องการของหน่วยงานเพื่อพิจารณาว่าบริการใดบ้างที่จำเป็นต้องใช้ดิจิทัลไอดีในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยมาตรฐานรัฐบาลดิจิทัลที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ ประกอบด้วย

(๖) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม (Digitalization: Digital ID – Overview)

(๗) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (Digitalization: Digital ID – Identity Proofing and Authentication)

(๘) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับนิติบุคคล (Digitalization: Digital ID – Identity Proofing and Authentication)

(๙) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติอื่น (Digitalization: Digital ID – Identity Proofing and Authentication)

(๑๐) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการออกดิจิทัลไอดีสำหรับบริการภาครัฐ (Digitalization: Digital ID – Government Issued ID)

สารบัญ

๑. ขอบข่าย ๑
๒. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Enrolment and Identity Proofing Requirements)... ๒
๒.๑ ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL) ๒
๒.๒ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Process Flow) ๓
๒.๓ ข้อกำหนดทั่วไป (General Requirements) ๕
๒.๔ ข้อกำหนดวิธีการพิสูจน์ตัวตน (Identity Proofing Method Requirements) ๗
๒.๕ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1) ๘
๒.๖ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2) ๙
๒.๗ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3) ๑๐
๒.๘ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (Summary of Requirements) ๑๒
๒.๙ ข้อกำหนดขั้นต่ำในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Minimum Requirements for Enrolment and Identity Proofing) ๑๔
๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล (Authentication Requirements) ๒๑
๓.๑ ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL) ๒๑
๓.๒ ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน (Authenticator and Verifier Requirements) ๒๒
๓.๓ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Lifecycle Management) ๒๒
๓.๔ การบริหารจัดการเซสชัน (Session Management) ๒๔
๓.๕ ภัยคุกคาม (Threats and Security Considerations) ๒๖
๓.๖ ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล (Minimum Requirement of Authentication). ๒๙
๔. การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล (Privacy Considerations) ๓๔
๔.๑ การจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization) ๓๔
๔.๒ เอกสารแจ้งข้อมูลและเอกสารแสดงความยินยอม (Privacy Notice and Consent) ๓๔
๔.๓ การคุ้มครองความเป็นส่วนบุคคล (Privacy Control) ๓๕
๔.๔ การใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น (Use Limitation) ๓๕
๔.๕ การแก้ไขข้อมูลส่วนบุคคล (Redress) ๓๕
๔.๖ การประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Risk Assessment) ๓๖
๔.๗ การดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Compliance) ๓๖
๕. แนวทางการนำไปใช้ (Usability Considerations) ๓๖

๕.๑ สำหรับผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP) ๓๖
๕.๒ สำหรับผู้ให้บริการภาครัฐ ๓๘
๕.๓ สำหรับแหล่งให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS) ๓๙
บรรณานุกรม ๔๐

สารบัญตาราง

ตารางที่ ๑ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี ๑๒
ตารางที่ ๒ แนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ..... ๑๕
ตารางที่ ๓ ภัยคุกคามและการบรรเทาภัยคุกคามที่อาจเกิดขึ้นในขั้นตอนการยืนยันตัวตน ๒๗
ตารางที่ ๔ แนวทางการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของกลุ่มการให้บริการภาครัฐ . ๓๐

สารบัญภาพ

รูปที่ ๑ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล ๓

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคง ปลอดภัยและมีธรรมาภิบาล ประกอบกับให้เป็นตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ และมีผลทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติ รวมทั้งให้หน่วยงานต่าง ๆ เกิดการพัฒนาทางเทคโนโลยีและส่งเสริมการใช้ธุรกรรมอิเล็กทรอนิกส์ให้สอดคล้องตามมาตรฐานที่กำหนด

เพื่อให้การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นไปตามวัตถุประสงค์ดังกล่าวข้างต้น โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๑๒ (๒) กำหนดให้หน่วยงานของรัฐจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน กระบวนการหรือการดำเนินงานทางดิจิทัลนั้นต้องทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ ประกอบมาตรา ๑๒ (๔) จัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ หมวด ๓/๑ ระบบการพิสูจน์และการยืนยันตัวตนทางดิจิทัล เพื่อกำกับดูแลการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้มีความน่าเชื่อถือและปลอดภัย จึงจำเป็นต้องกำหนดมาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

อาศัยอำนาจตามความในมาตรา ๔ และมาตรา ๗ (๓) (๙) มาตรา ๑๒ (๒) (๔) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะกรรมการพัฒนารัฐบาลดิจิทัลในคราวการประชุมครั้งที่ ๒/๒๕๖๔ วันที่๑๓ เดือนพฤษภาคม พ.ศ. ๒๕๖๔ จึงมีมติให้ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย"

ข้อ ๒ ในประกาศนี้

"บริการภาครัฐ" หมายความว่า การดำเนินการอย่างหนึ่งอย่างใดที่หน่วยงานของรัฐจัดทำหรือจัดให้มีขึ้นหรือที่มอบอำนาจให้เอกชนดำเนินการแทนเพื่ออำนวยความสะดวกหรือตอบสนองความต้องการของประชาชน

"ไอเดนทิตี" (identity หรือ ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด

"ดิจิทัลไอดี" (digital identity หรือ digital ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์

"ผู้พิสูจน์และยืนยันตัวตน" (identity provider) หมายความว่า บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่

(๑) รับลงทะเบียนและพิสูจน์ตัวตน และ

(๒) บริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้

"ผู้ให้บริการภาครัฐ" (relying party) หมายความว่า หน่วยงานของรัฐที่ให้บริการภาครัฐหรืออนุญาตให้เข้าถึงข้อมูลหรือระบบบริการภาครัฐ โดยอาศัยสิ่งที่ใช้ยืนยันตัวตนและผลการยืนยันตัวตนหรือสิ่งที่ใช้รับรองตัวตนจากผู้พิสูจน์และยืนยันตัวตน

"แหล่งให้ข้อมูลที่น่าเชื่อถือ" (authoritative source) หมายความว่า หน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง ซึ่งทำหน้าที่

(๑) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ

(๒) อนุญาตให้ผู้ให้บริการภาครัฐเข้าถึงข้อมูลที่น่าเชื่อถือหรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ

"ผู้สมัครใช้บริการ" (applicant) หมายความว่า บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

"ผู้ใช้บริการ" (subscriber) หมายความว่า ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

"การลงทะเบียน" (enrolment) หมายความว่า กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน

"การพิสูจน์ตัวตน" (identity proofing) หมายความว่า กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูลตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ

"การยืนยันตัวตน" (authentication) หมายความว่า กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน

"สิ่งที่ใช้ยืนยันตัวตน" (authenticator) หมายความว่า สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตนโดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

"สิ่งที่ใช้รับรองตัวตน" (credential) หมายความว่า เอกสาร วัตถุ หรือกลุ่มข้อมูล ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน

"คุณลักษณะ" (attribute) หมายความว่า ลักษณะหรือคุณสมบัติที่ใช้ระบุตัวบุคคล

หมวด ๑
บททั่วไป

ข้อ ๓ เพื่อให้การพิสูจน์และยืนยันตัวตนทางดิจิทัล มีความน่าเชื่อถือ พร้อมใช้ ตรวจสอบได้ และเป็นไปตามที่กฎหมายกำหนด โดยพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ ให้ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ ดำเนินการ ดังต่อไปนี้

(๑) จัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

(๒) จัดให้มีข้อตกลงในการดำเนินการและปฏิบัติตามข้อตกลงนั้น

(๓) ให้ความสำคัญและบริหารความเสี่ยงให้เหมาะสมกับระดับความเสี่ยงของบริการภาครัฐ โดยพิจารณาถึงผลกระทบที่อาจเกิดขึ้น เพื่อกำหนดวิธีการบรรเทาความเสียหายที่อาจเกิดขึ้น

ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือที่เป็นหน่วยงานของรัฐ ให้จัดทำธรรมาภิบาลข้อมูลภาครัฐและดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐที่เกี่ยวข้องกับกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐด้วย

หมวด ๒
การพิสูจน์และยืนยันตัวตนทางดิจิทัล

ข้อ ๔ ให้ผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังต่อไปนี้

(๑) กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัล และจัดสรรบุคลากร ระบบ เทคโนโลยีที่จำเป็น ให้สอดคล้องกับระดับความน่าเชื่อถือ

(๒) กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่ที่ได้รับการฝึกอบรมหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

(๓) กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐให้ดำเนินการตามข้อกำหนดการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามมาตรฐานและหลักเกณฑ์นี้ หากผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนให้ดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๔) จัดให้มีการขอความยินยอมของผู้สมัครใช้บริการ โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย

(๕) จัดให้มีการแสดงตนและรวบรวมข้อมูลเพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

(๖) ตรวจสอบหลักฐานแสดงตนของผู้สมัครใช้บริการ เพื่อตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน และตรวจสอบข้อมูลในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

(๗) ตรวจสอบตัวบุคคลของผู้สมัครใช้บริการที่แสดงหลักฐานแสดงตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจตรวจสอบช่องทางติดต่อว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อ และสามารถติดต่อหรือส่งข้อมูลไปยังผู้สมัครใช้บริการผ่านช่องทางดังกล่าวได้จริง

(๘) เก็บรักษาข้อมูลและหลักฐานแสดงตน รวมถึงภาพและเสียง (ถ้ามี) และการบันทึกเหตุการณ์และรายละเอียดการทำธุรกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยระยะเวลาการเก็บรักษาและการบันทึกดังกล่าวให้เป็นไปตามกฎหมาย ข้อบังคับ หรือแนวนโยบายที่เกี่ยวข้อง

(๙) ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๑๐) ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

ข้อ ๕ ให้ผู้ให้บริการภาครัฐดำเนินการ ดังต่อไปนี้

(๑) กำหนดความต้องการและระบบของหน่วยงานที่ต้องการใช้ดิจิทัลไอดี

(๒) ประเมินความเสี่ยงเพื่อพิจารณาถึงผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์หรือยืนยันตัวตนผิดพลาด

(๓) นำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือทั้งระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๔) เลือกรูปแบบ และวิธีการลงทะเบียน การพิสูจน์ตัวตนและยืนยันตัวตนทางดิจิทัล รวมถึงกำหนดเงื่อนไขให้สอดคล้องตามข้อกำหนดในแต่ละระดับความน่าเชื่อถือตามกลุ่มให้บริการภาครัฐ และแจ้งให้ทราบล่วงหน้า

ข้อ ๖ ให้แหล่งให้ข้อมูลที่น่าเชื่อถือตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

บทเฉพาะกาล

ข้อ ๗ ในระยะเริ่มแรก มิให้นำมาตรฐานและหลักเกณฑ์ตามประกาศนี้มาใช้บังคับกับผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ จนกว่าจะพ้นกำหนดสองปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

ประกาศ ณ วันที่ ๑๖ กันยายน ๒๕๖๔

(นายตอน ปรมัตถ์วินัย)
รองนายกรัฐมนตรี
ประธานกรรมการพัฒนารัฐบาลดิจิทัล

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

๑. ขอบข่าย

มาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ เป็นแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย เป็นข้อกำหนดและแนวทางในการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ใช้บริการที่ต้องการใช้บริการภาครัฐด้วยดิจิทัลไอดี เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยอ้างอิงข้อกำหนด ดังนี้

(๗) มาตรฐาน NIST Special Publication 800-63-3 – Digital Identity Guidelines [๑]

(๘) มาตรฐาน NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing [๒]

(๙) มาตรฐาน NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management [๓]

(๑๐) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔]

(๑๑) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]

(๑๒) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

(๑๓) ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน [๙]

(๑๔) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร [๑๐]

ในมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) [๑] มีดังนี้

– “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ที่ต้องปฏิบัติตาม

– “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)

– “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

การลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Enrolment and Identity Proofing)

๒. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Enrolment and Identity Proofing Requirements)

การลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลต้องทำให้มั่นใจได้ว่าผู้สมัครใช้บริการเป็นบุคคลที่กล่าวอ้างจริง โดยผ่านการแสดงตน (presentation) การตรวจสอบหลักฐานแสดงตน (validation) และการตรวจสอบตัวบุคคล (verification) โดยผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงความสมดุลระหว่างความเป็นส่วนบุคคลและความต้องการที่จะใช้ข้อมูลของผู้ใช้บริการ เพื่อกำหนดเป็นคุณลักษณะขั้นต่ำที่จำเป็น (attribute) ในการพิสูจน์ตัวตนทางดิจิทัล เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน (laser code)

๒.๑ ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของไอเดนทิตี คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ การกำหนดระดับความน่าเชื่อถือของไอเดนทิตีที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด โดยระดับความน่าเชื่อถือของไอเดนทิตี แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาและตรวจสอบหลักฐานแสดงตนหรือไม่ก็ได้ ทั้งนี้ไม่มีข้อกำหนดในการแสดงตนและตรวจสอบตัวบุคคลโดยผู้พิสูจน์และยืนยันตัวตน เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

กำหนดให้มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาหลักฐานแสดงตน โดยผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบกับแหล่งให้ข้อมูลที่น่าเชื่อถือว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง รวมถึงตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า หรือแบบไม่พบเห็นต่อหน้า

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐที่ให้บริการที่ต้องการระดับ IAL1 ได้ หากผู้ใช้บริการให้ความยินยอม เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

เพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ IAL2 ด้วยการพิจารณาหลักฐานแสดงตนเพิ่มเติมและการตรวจสอบข้อมูลชีวมิติ เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวงการลงทะเบียนซ้ำ หรือความเสียหายอื่น ๆ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้เฉพาะแบบพบเห็นต่อหน้า ซึ่งรวมถึงแบบเสมือนพบเห็นต่อหน้า

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐที่ให้บริการที่ต้องการระดับ IAL1 และ IAL2 ได้ หากผู้ใช้บริการให้ความยินยอม เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

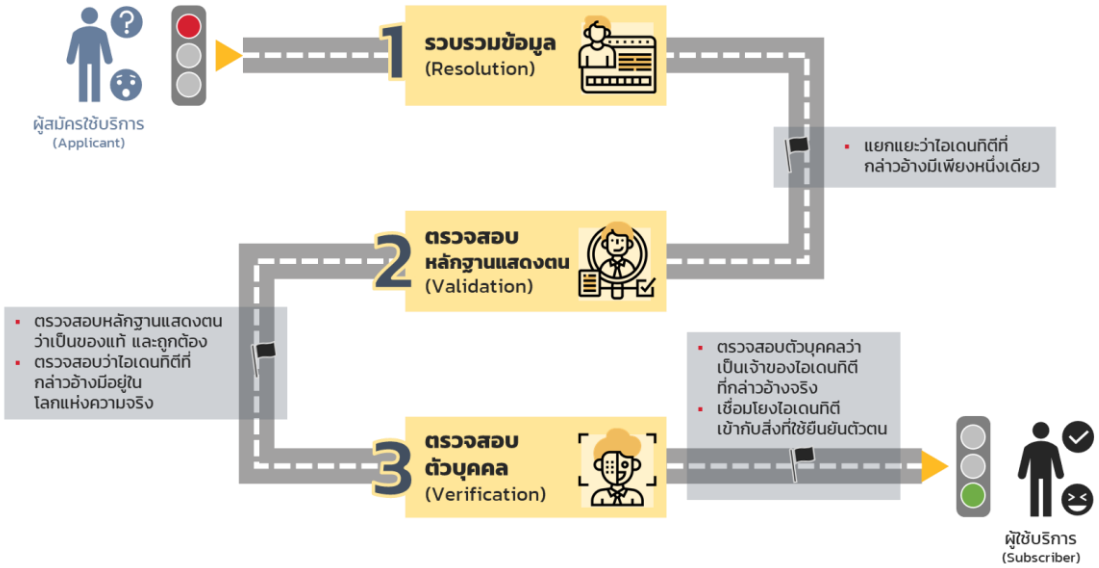
๒.๒ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Process Flow)

เพื่อให้ขั้นตอนการรวบรวมและตรวจสอบข้อมูลหลักฐานแสดงตนของผู้สมัครใช้บริการมีคุณภาพเพียงพอที่จะมั่นใจว่า (๑) ผู้สมัครใช้บริการมีตัวตนจริงและมีเพียงหนึ่งเดียว (๒) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ (๓) ผู้สมัครใช้บริการเป็นเจ้าของหลักฐานที่นำมาแสดง มีกระบวนการดำเนินการ ดังนี้

(๑) การรวบรวมข้อมูลเพื่อระบุตัวตน เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมคุณลักษณะและหลักฐานแสดงตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล ทั้งนี้ การระบุตัวตนที่ดีควรใช้ชุดของคุณลักษณะเท่าที่จำเป็นในการแยกแยะไอเดนทิตีของผู้สมัครใช้บริการแต่ละราย

(๒) การตรวจสอบหลักฐานแสดงตน เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน รวมถึงตรวจสอบข้อมูลที่อยู่ในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

(๓) การตรวจสอบตัวบุคคล เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนตรวจสอบตัวบุคคลที่แสดงหลักฐานแสดงตน ว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจมีการตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการที่ได้ให้ไว้ในขั้นตอนการลงทะเบียนว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อจริง รวมถึงสามารถติดต่อหรือส่งข้อมูลข่าวสารสำคัญไปยังผู้สมัครใช้บริการผ่านช่องทางดังกล่าวได้จริง



รูปที่ ๑ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล

ที่มา: ปรับปรุงจาก (NIST, NIST Special Publication 800-63A – Digital Identity Guidelines - Enrollment and Identity Proofing, 2017) [๒]

จากรูปที่ ๑ แสดงให้เห็นขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล มีทั้งหมด ๓ ขั้นตอน ได้แก่

(๑) รวบรวมข้อมูลเพื่อระบุตัวตน (resolution)

การรวบรวมข้อมูลเพื่อระบุตัวตนมีจุดมุ่งหมายเพื่อแยกแยะว่าไอเดนทิตีที่กล่าวอ้างมีเพียงหนึ่งเดียว โดยใช้ชุดของคุณลักษณะที่ใช้ระบุตัวตนให้น้อยที่สุดเท่าที่จำเป็นเพื่อแยกแยะไอเดนทิตีที่กล่าวอ้างออกจากไอเดนทิตีอื่น ซึ่งการรวบรวมข้อมูลเพื่อระบุตัวตนถือเป็นจุดเริ่มต้นของกระบวนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล เช่น

(๑.๑) รวบรวมข้อมูลส่วนบุคคลจากผู้สมัครใช้บริการ เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน อีเมล หมายเลขโทรศัพท์เคลื่อนที่

(๑.๒) รวบรวมหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชนหรือหนังสือเดินทาง โดยอาจมีการทำสำเนาหรือถ่ายภาพไว้เป็นหลักฐาน

(๒) ตรวจสอบหลักฐานแสดงตน (validation)

การตรวจสอบหลักฐานแสดงตนมีจุดมุ่งหมายเพื่อรวบรวมหลักฐานการระบุตัวตนที่เหมาะสมที่สุดจากผู้สมัครใช้บริการเพื่อแสดงถึงความเป็นของแท้ สมบูรณ์ และถูกต้อง ซึ่งขั้นตอนของการตรวจสอบหลักฐานแสดงตน ประกอบด้วย การรวบรวมหลักฐานแสดงตนที่เหมาะสม การยืนยันหลักฐานแสดงตนว่าเป็นของแท้ และการยืนยันข้อมูลของหลักฐานแสดงตนว่าถูกต้อง เป็นปัจจุบัน และไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง เช่น

(๒.๑) ตรวจสอบข้อมูลที่ได้จากการรวบรวมข้อมูลตามข้อ (๑) กับแหล่งให้ข้อมูลที่น่าเชื่อถือโดยผู้พิสูจน์และยืนยันตัวตนต้องประเมินข้อมูลที่ได้รับจากผู้สมัครใช้บริการว่าตรงกัน

(๒.๒) ตรวจสอบสำเนาหรือภาพถ่ายของหลักฐานแสดงตนว่าไม่มีการปลอมแปลงแก้ไข เช่น เลขประจำตัวประชาชนที่อยู่ในสำเนาหรือภาพถ่ายต้องอยู่ในรูปแบบมาตรฐานที่กรมการปกครองกำหนด

(๒.๓) ตรวจสอบข้อมูลกับแหล่งออกหลักฐานแสดงตนว่าตรงกัน

(๓) ตรวจสอบตัวบุคคล (verification)

การตรวจสอบตัวบุคคลมีจุดมุ่งหมายเพื่อยืนยันและเชื่อมโยงระหว่างไอเดนทิตีที่กล่าวอ้างกับบุคคลที่ยื่นหลักฐานแสดงตนว่าตรงกันและมีตัวตนอยู่ในโลกแห่งความจริง เช่น

(๓.๑) ให้ผู้สมัครใช้บริการถ่ายภาพตนเอง เพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรม (liveness check) และตรวจสอบกับหลักฐานแสดงตนว่าตรงกัน

(๓.๒) นำภาพถ่ายจากหลักฐานแสดงตนเทียบกับภาพถ่ายของผู้สมัครใช้บริการว่าตรงกัน

(๓.๓) อาจมีการส่งรหัสการลงทะเบียนไปยังหมายเลขโทรศัพท์เคลื่อนที่ของผู้สมัครใช้บริการ โดยให้ผู้สมัครใช้บริการยืนยันรหัสการลงทะเบียนกลับมายังผู้พิสูจน์และยืนยันตัวตน โดยผู้พิสูจน์และยืนยันตัวตนเป็นผู้ยืนยันว่ารหัสดังกล่าวตรงกัน เพื่อเป็นการตรวจสอบว่าหมายเลขโทรศัพท์เคลื่อนที่นั้นเป็นของผู้สมัครใช้บริการจริง

๒.๓ ข้อกำหนดทั่วไป (General Requirements)

ข้อกำหนดทั่วไปสำหรับผู้พิสูจน์และยืนยันตัวตน ดำเนินการพิสูจน์ตัวตนของผู้สมัครใช้บริการที่มาขอใช้บริการว่าเป็นบุคคลรายนั้นจริง เพื่อป้องกันการทุจริตจากการปลอมแปลงหรือใช้ข้อมูลของบุคคลอื่นในการใช้บริการภาครัฐ ดังนี้

(๑) ต้องจัดให้ผู้สมัครใช้บริการแสดงตนและตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและหลักฐานแสดงตนที่ได้รับจากผู้สมัครใช้บริการ รวมถึง ตรวจสอบว่าบุคคลที่มาสมัครใช้บริการภาครัฐเป็นบุคคลเดียวกันกับบุคคลในหลักฐานแสดงตน

(๒) ต้องบริหารความเสี่ยงให้เหมาะสมและสอดคล้องกับความเสี่ยงของบริการภาครัฐ โดยวิธีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้าและแบบเสมือนพบเห็นต่อหน้าอาจมีความเสี่ยงสูงกว่าแบบพบเห็นต่อหน้า จึงต้องพิสูจน์ตัวตนในระดับที่เข้มข้นกว่า รวมถึงจัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อบริหารความเสี่ยงให้มีประสิทธิภาพมากขึ้น

(๓) ต้องกำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่หรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในของผู้พิสูจน์และยืนยันตัวตนหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง นอกจากนี้ ต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

ทั้งนี้ ข้อกำหนดทั่วไปสำหรับผู้พิสูจน์และยืนยันตัวตนดำเนินการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ หรือ ๓ ดังนี้

(๑) การพิสูจน์ตัวตนต้องไม่เป็นการประเมินถึงความเหมาะสม หรือการกำหนดสิทธิในการเข้าถึงบริการหรือสิทธิประโยชน์ต่าง ๆ

(๒) การรวบรวมข้อมูลส่วนบุคคลต้องรวบรวมให้น้อยที่สุดเท่าที่จำเป็น เพื่อตรวจสอบไอเดนทิตีที่กล่าวอ้างและเชื่อมโยงกับหลักฐานแสดงตนของผู้สมัครใช้บริการได้อย่างเหมาะสมสำหรับการรวบรวมข้อมูลเพื่อระบุตัวตน การตรวจสอบหลักฐานแสดงตน และการตรวจสอบตัวบุคคล ซึ่งอาจตรวจสอบหลักฐานแสดงตนกับแหล่งให้ข้อมูลที่น่าเชื่อถือและส่งให้ผู้ให้บริการภาครัฐใช้ในการตัดสินใจให้สิทธิเข้าใช้บริการ

(๓) ต้องแจ้งวัตถุประสงค์อย่างชัดเจนของการรวบรวมและจัดเก็บรักษาข้อมูลส่วนบุคคลที่ใช้สำหรับการพิสูจน์ตัวตนเท่าที่จำเป็น รวมถึงระบุคุณลักษณะที่ขึ้นอยู่กับความสมัครใจหรือคุณลักษณะที่จำเป็นต่อกระบวนการพิสูจน์ตัวตน และผลที่ตามมาหากผู้สมัครใช้บริการไม่แสดงคุณลักษณะดังกล่าว

(๔) ไม่นำคุณลักษณะที่รวบรวมและจัดเก็บในกระบวนการพิสูจน์ตัวตนไปใช้กับวัตถุประสงค์อื่นนอกเหนือจากการพิสูจน์ตัวตน การยืนยันตัวตน หรือปฏิบัติตามที่กฎหมายกำหนด โดยผู้พิสูจน์และยืนยันตัวตนต้องมีมาตรการในการรับมือกับความเสี่ยงที่อาจเกิดขึ้นกับความเป็นส่วนบุคคล เพื่อป้องกันไม่ให้เกิดการทำผิดกฎหมาย เว้นแต่ผู้พิสูจน์และยืนยันตัวตนได้แจ้งให้ผู้สมัครใช้บริการทราบอย่างชัดเจน และได้รับความยินยอมให้นำคุณลักษณะไปใช้กับ

วัตถุประสงค์อื่น ๆ ทั้งนี้ผู้พิสูจน์และยืนยันตัวตนต้องไม่กำหนดการให้ความยินยอมให้นำคุณลักษณะไปใช้กับวัตถุประสงค์อื่น ๆ เป็นเงื่อนไขในการให้บริการ

(๕) ต้องจัดให้มีกลไกสำหรับการแก้ไขข้อร้องเรียนหรือปัญหาของผู้สมัครใช้บริการที่เกิดขึ้นจากการพิสูจน์ตัวตน โดยกลไกดังกล่าวต้องให้ผู้สมัครใช้บริการค้นหาและใช้งานได้ง่าย ทั้งนี้ผู้พิสูจน์และยืนยันตัวตนต้องประเมินประสิทธิภาพของกลไกต่าง ๆ ในการแก้ไขข้อร้องเรียนหรือปัญหาต่าง ๆ ที่เกิดขึ้น

(๖) ต้องดำเนินการตามนโยบายหรือแนวปฏิบัติของการลงทะเบียนและพิสูจน์ตัวตน ซึ่งระบุขั้นตอนของการตรวจสอบไอเดนทิตี โดยแนวปฏิบัติดังกล่าวต้องประกอบด้วยมาตรการควบคุมของผู้พิสูจน์และยืนยันตัวตนที่ต้องดำเนินการอย่างไร หากมีข้อผิดพลาดในการพิสูจน์ตัวตนที่ทำให้ผู้สมัครใช้บริการลงทะเบียนไม่สำเร็จ เช่น จำนวนครั้งที่อนุญาตให้ลองลงทะเบียนใหม่ ทางเลือกของการพิสูจน์ตัวตน (เช่น ระบบออนไลน์ล้มเหลว) หรือมาตรการรับมือการฉ้อโกงเมื่อตรวจพบความผิดปกติ

(๗) ต้องจัดเก็บบันทึก รวมถึงบันทึกการตรวจสอบ (audit log) ของรายละเอียดทุกขั้นตอนของการตรวจสอบไอเดนทิตีของผู้สมัครใช้บริการ ต้องบันทึกประเภทหลักฐานแสดงตนที่นำมาแสดงตนในขั้นตอนของการพิสูจน์ตัวตน และต้องดำเนินการตามกระบวนการบริหารจัดการความเสี่ยง รวมถึงการประเมินความเสี่ยงด้านความเป็นส่วนบุคคลและความมั่นคงปลอดภัยเพื่อกำหนด ดังนี้

(๗.๑) ขั้นตอนเพิ่มเติมใด ๆ ที่ใช้ในการตรวจสอบไอเดนทิตีของผู้สมัครใช้บริการ นอกเหนือจากข้อกำหนดที่ต้องปฏิบัติตามซึ่งระบุไว้ในมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้

(๗.๒) ข้อมูลส่วนบุคคล รวมถึงข้อมูลชีวมิติ รูปภาพ ภาพสแกน หรือสำเนาของหลักฐานแสดงตนอื่น ๆ ที่ผู้พิสูจน์และยืนยันตัวตนต้องจัดเก็บไว้เป็นบันทึกของการพิสูจน์ตัวตน

(๗.๓) ระยะเวลาของการจัดเก็บบันทึกของการพิสูจน์ตัวตนให้เป็นไปตามกฎหมาย กฎระเบียบหรือนโยบายต่าง ๆ ที่เกี่ยวข้อง

(๘) ข้อมูลส่วนบุคคลทั้งหมดที่ได้รวบรวมมาจากกระบวนการลงทะเบียน ต้องมีการปกป้องเพื่อให้มั่นใจได้ว่ามีการรักษาความลับ (confidentiality) มีความครบถ้วน ถูกต้อง สมบูรณ์ (integrity) และระบุแหล่งที่มาของข้อมูล (attribution of the information source)

(๙) การทำธุรกรรมที่เกี่ยวกับการพิสูจน์ตัวตนทั้งหมด รวมถึงธุรกรรมที่เกี่ยวข้องกับบุคคลที่สาม ต้องดำเนินการผ่านช่องทางการติดต่อสื่อสารที่มีความมั่นคงปลอดภัย

(๑๐) ควรมีมาตรการเพิ่มเติมเพื่อบรรเทาการฉ้อโกงและเพิ่มความน่าเชื่อถือในการพิสูจน์ตัวตน เช่น การตรวจสอบตำแหน่งทางภูมิศาสตร์ การตรวจสอบอุปกรณ์ การตรวจสอบลักษณะและพฤติกรรมของผู้สมัครใช้บริการ และต้องประเมินความเสี่ยงด้านความเป็นส่วนบุคคลสำหรับมาตรการดังกล่าวข้างต้น ซึ่งการประเมินความเสี่ยงดังกล่าวต้องรวมถึงการบรรเทาความเสี่ยง เช่น การยอมรับหรือถ่ายโอนความเสี่ยง การจัดเก็บในระยะเวลาที่จำกัด การจำกัดการใช้ข้อมูลและการแจ้งข้อมูลรวมถึงการใช้เทคโนโลยีเพื่อช่วยบรรเทาความเสี่ยง เช่น การเข้ารหัส (cryptography) และการจัดทำเอกสารตามข้อกำหนดที่ ๒.๓ (๗)

(๑๑)เมื่อกระบวนการลงทะเบียนและพิสูจน์ตัวตนสิ้นสุดลง ต้องกำจัดหรือทำลายข้อมูลอ่อนไหว (sensitive data) รวมถึงข้อมูลส่วนบุคคล หรือการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ตลอดช่วงระยะเวลาของเก็บรักษาข้อมูล

๒.๔ ข้อกำหนดวิธีการพิสูจน์ตัวตน (Identity Proofing Method Requirements)

ต้องนำข้อมูลและหลักฐานแสดงตนมาตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบัน รวมถึงตรวจสอบตัวบุคคลว่าเป็นผู้สมัครใช้บริการรายนั้นจริง โดยต้องดำเนินการดังนี้

๒.๔.๑ การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) กรณีผู้สมัครใช้บริการแสดงบัตรประจำตัวประชาชน ต้องตรวจสอบสถานะของข้อมูลและบัตรประจำตัวประชาชนของผู้สมัครใช้บริการที่เป็นปัจจุบันผ่านระบบให้บริการของแหล่งให้ข้อมูลที่น่าเชื่อถือ เพื่อทราบสถานะของข้อมูลและบัตรประจำตัวประชาชน

(๓) กรณีผู้สมัครใช้บริการแสดงหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ต้องตรวจสอบความถูกต้อง ความแท้จริงของข้อมูลและหลักฐานแสดงตนด้วยเครื่องมืออิเล็กทรอนิกส์ เพื่อป้องกันการปลอมแปลงข้อมูลบนหน้าหลักฐานแสดงตน ทั้งนี้ หากผู้สมัครใช้บริการไม่มีหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ หรือมีเหตุจำเป็นที่หลักฐานแสดงตนที่มีข้อมูลอิเล็กทรอนิกส์บกพร่อง ให้บริหารความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสมและรัดกุม

(๔) กรณีผู้สมัครใช้บริการให้ช่องทางการติดต่อเป็นหมายเลขโทรศัพท์เคลื่อนที่ หรืออีเมล ต้องตรวจสอบหมายเลขโทรศัพท์เคลื่อนที่ หรืออีเมลดังกล่าวของผู้สมัครใช้บริการว่าสามารถติดต่อได้จริง

(๕) กรณีเลือกใช้วิธีการตรวจสอบลักษณะที่ปรากฏเทียบกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) ต้องตรวจสอบว่าตรงกับลักษณะที่ปรากฏของผู้สมัครใช้บริการเพื่อยืนยันว่าเป็นเจ้าของหลักฐานแสดงตนดังกล่าวจริง ทั้งนี้ กรณีผู้สมัครใช้บริการแสดงหลักฐานแสดงตนที่มีข้อมูลอิเล็กทรอนิกส์ ควรใช้รูปถ่ายที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์จากหลักฐานแสดงตนดังกล่าว เพื่อป้องกันการปลอมแปลงรูปถ่ายบนหน้าหลักฐานแสดงตน

(๖) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ (biometric comparison) เช่น ภาพใบหน้า หรือลายนิ้วมือ ต้องตรวจสอบเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตนว่าตรงกับผู้สมัครใช้บริการรายนั้นจริง

๒.๔.๒ การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) ต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบที่มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานแสดงตนของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้า

(๓) กรณีเลือกใช้วิธีการตรวจสอบลักษณะที่ปรากฏจากรูปถ่ายของผู้สมัครใช้บริการเทียบกับรูปถ่ายจากหลักฐานแสดงตน ต้องตรวจสอบว่าตรงกับลักษณะที่ปรากฏของผู้สมัครใช้บริการเพื่อยืนยันว่าเป็นเจ้าของหลักฐานแสดงตนดังกล่าวจริง

(๔) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ เช่น ภาพใบหน้า หรือลายนิ้วมือ อาจใช้เทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมผู้สมัครใช้บริการ (liveness detection) และเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการ เพื่อพิสูจน์ว่าเป็นผู้สมัครใช้บริการรายนั้นจริงทดแทนการพบเห็นต่อหน้า ถ้าไม่สามารถสังเกตพฤติกรรมของผู้สมัครใช้บริการ ต้องกำหนดกระบวนการหรือแนวทางการบริหารความเสี่ยงเพิ่มเติมเพื่อลดความเสี่ยงจากกรณีทุจริตต่าง ๆ ได้

๒.๔.๓ การพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) ต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบที่มีความน่าเชื่อถือและมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานแสดงตนของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๓) ต้องจัดให้มีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการลงทะเบียนและพิสูจน์ตัวตน

๒.๕ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ ดังนี้

(๑) รวบรวมข้อมูลส่วนบุคคลเพื่อระบุตัวตนของผู้สมัครใช้บริการหรือไม่ก็ได้

(๒) กรณีขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ มีดังนี้

(๒.๑) บัตรประจำตัวประชาชน **หรือ**

(๒.๒) หนังสือเดินทาง **หรือ**

(๒.๓) หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

(๓) ตรวจสอบข้อมูลหรือหลักฐานแสดงตนตามข้อ ๒.๕ (๒) ว่าเป็นของแท้ และถูกต้อง

(๔) ตรวจสอบช่องทางการติดต่อว่าสามารถติดต่อผู้สมัครใช้บริการได้

๒.๖ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ ดังนี้

(๑) ต้องรองรับวิธีการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** ไม่พบเห็นต่อหน้า ทั้งนี้ควรจัดให้มีการพิสูจน์ตัวตนทั้งสองรูปแบบสำหรับการแสดงตนของผู้สมัครใช้บริการ

(๒) การรวบรวมข้อมูลเพื่อระบุตัวตน

(๒.๑) ต้องรวบรวมข้อมูลส่วนบุคคลของผู้สมัครใช้บริการเท่าที่จำเป็น เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล ซึ่งอาจรวมถึงการรวบรวมคุณลักษณะ เพื่อช่วยในการค้นหาข้อมูล

(๒.๒) อาจใช้การยืนยันด้วยชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (knowledge-based verification: KBV)

(๓) ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ ดังนี้

(๓.๑) บัตรประจำตัวประชาชน **หรือ**

(๓.๑) หนังสือเดินทาง **หรือ**

(๓.๑) หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

(๔) การตรวจสอบหลักฐานแสดงตน

(๔.๑) ต้องตรวจสอบหลักฐานแสดงตนตาม ๒.๖ (๓) โดยใช้เจ้าหน้าที่หรือเทคโนโลยีที่เหมาะสมว่าเป็นของแท้

(๔.๑) ต้องตรวจสอบข้อมูลของหลักฐานแสดงตนตาม ๒.๖ (๓) โดยเปรียบเทียบกับข้อมูลจากแหล่งให้ข้อมูลที่น่าเชื่อถือว่ามีความถูกต้อง

(๕) การตรวจสอบตัวบุคคล

(๕.๑) ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน **หรือ** เปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน

(๕.๑) อาจบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด (non-repudiation) และการตรวจสอบอีกครั้งในกรณีจำเป็น (re-proofing)

(๖) การตรวจสอบช่องทางการติดต่อ

(๖.๑) ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้จริง เช่น การตรวจสอบอีเมลด้วยวิธีการยืนยันทางอีเมล การตรวจสอบหมายเลขโทรศัพท์เคลื่อนที่ด้วยรหัสผ่านแบบใช้ครั้งเดียว (OTP) หรือวิธีการยืนยันทาง SMS

๒.๗ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ ดังนี้

(๑) ต้องพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** เสมือนพบเห็นต่อหน้า ทั้งนี้ควรจัดให้มีการพิสูจน์ตัวตนทั้งสองรูปแบบสำหรับการแสดงตนเพื่อระบุตัวตนของผู้สมัครใช้บริการ โดยมีข้อกำหนด ดังนี้

(๑.๑) ข้อกำหนดของการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๑.๑.๑) ต้องมีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรมทำหน้าที่สังเกตสิ่งผิดปกติบนร่างกายของผู้สมัครใช้บริการ (เช่น ใบหน้า นิ้วมือ) และดำเนินการตรวจสอบตามกระบวนการพิสูจน์ตัวตน

(๑.๑.๒) ต้องรวบรวมข้อมูลชีวมิติในลักษณะที่มั่นใจว่าข้อมูลชีวมิติดังกล่าวถูกรวบรวมจากผู้สมัครใช้บริการ และไม่ใช่จากบุคคลอื่น

(๑.๒) ข้อกำหนดของการพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้า

(๑.๒.๑) ต้องเฝ้าสังเกตผู้สมัครใช้บริการตลอดเวลาของการพิสูจน์ตัวตน โดยที่ผู้สมัครใช้บริการต้องไม่ออกไปจากการสื่อสาร เช่น การเฝ้าสังเกตผู้สมัครใช้บริการด้วยการส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง (high resolution video transmission)

(๑.๒.๒) ต้องมีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการพิสูจน์ตัวตน เช่น การส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง

(๑.๒.๓) เจ้าหน้าที่ต้องสามารถมองเห็นพฤติกรรมทั้งหมดของผู้สมัครใช้บริการระหว่างช่วงเวลาของการพิสูจน์ตัวตนได้อย่างชัดเจน

(๑.๒.๔) ต้องตรวจสอบหลักฐานแสดงตนด้วยวิธีการทางอิเล็กทรอนิกส์ โดยใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือวิธีการที่เทียบเท่า เช่น การตรวจสอบลายมือชื่อที่ออกหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ และใช้เครื่องมืออุปกรณ์ของผู้พิสูจน์และยืนยันตัวตนทั้งหมด

(๑.๒.๕) ต้องฝึกอบรมเจ้าหน้าที่เพื่อให้สามารถตรวจหาความผิดปกติที่อาจเกิดขึ้นในการพิสูจน์ตัวตน และดำเนินการได้อย่างเหมาะสม

(๑.๒.๖) ต้องติดตั้งระบบตรวจจับการบุกรุกทางกายภาพที่เหมาะสมกับสภาพแวดล้อมของสถานที่ตั้ง เช่น เครื่องให้บริการอัตโนมัติ (kiosk) ต้องตั้งอยู่ในพื้นที่ที่จำกัดหรือพื้นที่ที่มีการรักษาความมั่นคงปลอดภัย

(๑.๒.๗) ต้องตรวจสอบให้มั่นใจว่าการติดต่อสื่อสารทั้งหมดเกิดขึ้นผ่านช่องทางการสื่อสารเฉพาะที่มีการป้องกัน

(๒) การรวบรวมข้อมูลเพื่อระบุตัวตน

(๒.๑) ข้อกำหนดเช่นเดียวกับ IAL2

(๓) ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ โดยมีทางเลือก ดังนี้

(๓.๑) บัตรประจำตัวประชาชนและหนังสือเดินทาง **หรือ**

(๓.๒) ใช้การตรวจสอบหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ**

(๓.๓) บัตรประจำตัวประชาชนและแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป

(๔) การตรวจสอบหลักฐานแสดงตน

(๔.๑) ข้อกำหนดเช่นเดียวกับ IAL2

(๕) การตรวจสอบตัวบุคคล

(๕.๑) ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน

(๕.๒) ต้องบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด และการตรวจสอบอีกครั้งในกรณีจำเป็น

(๖) การตรวจสอบช่องทางการติดต่อ

(๖.๑) ข้อกำหนดเช่นเดียวกับ IAL2

๒.๘ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (Summary of Requirements)

ข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี สรุปได้ดังตารางที่ ๑

ตารางที่ ๑ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

ข้อกำหนด	IAL1	IAL2	IAL3
การแสดงตน	ไม่มีข้อกำหนด	ต้องรองรับวิธีการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** ไม่พบเห็นต่อหน้า	ต้องพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** เสมือนพบเห็นต่อหน้า
การรวบรวมข้อมูลเพื่อระบุตัวตน	รวบรวมข้อมูลเพื่อระบุตัวตนหรือไม่ก็ได้	- ต้องรวบรวมข้อมูลเพื่อระบุตัวตน - อาจใช้ชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (knowledge-based verification : KBV)	เช่นเดียวกับ IAL2
การขอหลักฐานแสดงตน	ขอหลักฐานแสดงตนที่ยังไม่หมดอายุหรือไม่ก็ได้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ - ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป

ตารางที่ ๑ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

(ต่อ)

ข้อกำหนด	IAL1	IAL2	IAL3
การตรวจสอบหลักฐานแสดงตน	ตรวจสอบและเปรียบเทียบหลักฐานแสดงตนที่ยังไม่หมดอายุว่าเป็นของแท้และถูกต้องหรือไม่ก็ได้	- ต้องตรวจสอบหลักฐานแสดงตนโดยใช้เจ้าหน้าที่หรือเทคโนโลยีที่เหมาะสมว่าเป็นของแท้ - ต้องตรวจสอบข้อมูลของหลักฐานแสดงตนโดยเปรียบเทียบกับข้อมูลจากแหล่งให้ข้อมูลที่น่าเชื่อถือว่ามีความถูกต้อง	เช่นเดียวกับ IAL2
การตรวจสอบตัวบุคคล	ไม่ตรวจสอบตัวบุคคล	ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย - เปรียบเทียบลักษณะที่ปรากฏเทียบกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) **หรือ** - เปรียบเทียบภาพใบหน้าหรือลายนิ้วมือเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย - เปรียบเทียบภาพใบหน้าหรือลายนิ้วมือเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)
การรวบรวมข้อมูลชีวมิติ	ไม่มีข้อกำหนด	บันทึกตัวอย่างข้อมูลชีวมิติ (biometric sample) หรือไม่ก็ได้	ต้องบันทึกตัวอย่างข้อมูลชีวมิติ (biometric sample)
การตรวจสอบช่องทางการติดต่อ	ตรวจสอบช่องทางการติดต่อว่าสามารถติดต่อได้ - หมายเลขโทรศัพท์เคลื่อนที่ **หรือ** - อีเมล	ต้องตรวจสอบช่องทางการติดต่อ - หมายเลขโทรศัพท์เคลื่อนที่ **หรือ** - อีเมล	เช่นเดียวกับ IAL2

๒.๙ ข้อกำหนดขั้นต่ำในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Minimum Requirements for Enrolment and Identity Proofing)

ผู้พิสูจน์และยืนยันตัวตนระบุข้อกำหนดในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลให้เป็นไปตามกลุ่มการให้บริการภาครัฐ ทั้ง ๔ กลุ่ม [๘] โดยต้องประเมินความต้องการของหน่วยงาน ความเสี่ยง และระดับความน่าเชื่อถือ โดยเลือกวิธีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลที่เหมาะสม เพื่อให้ขั้นตอนการรวบรวม และตรวจสอบข้อมูลหลักฐานแสดงตนของผู้สมัครใช้บริการ มีคุณภาพเพียงพอที่จะให้มั่นใจว่า (๑) ผู้สมัครใช้บริการมีตัวตนจริงและมีเพียงหนึ่งเดียว (๒) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ (๓) ผู้สมัครใช้บริการเป็นเจ้าของหลักฐานที่นำมาแสดง

ข้อกำหนดขั้นต่ำในการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีสำหรับการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล จำแนกตามกลุ่มการให้บริการภาครัฐ ดังนี้

(๑) กลุ่มการให้บริการข้อมูลพื้นฐาน จัดเป็นบริการที่ไม่มีความเสี่ยงหรือมีความเสี่ยงต่ำ จึง**ไม่จำเป็นต้องใช้ดิจิทัลไอดี**

(๒) กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ จัดเป็นบริการที่มีความเสี่ยงต่ำ สามารถใช้การพิสูจน์ตัวตนในระดับความน่าเชื่อถือของไอเดนทิตี **อย่างน้อยระดับที่ ๑**

(๓) กลุ่มการให้บริการธุรกรรม จัดเป็นบริการที่มีความเสี่ยงปานกลางถึงสูง เนื่องจากการให้บริการดังกล่าว ผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบความถูกต้อง ความแท้จริงของผู้สมัครใช้บริการ โดยการตรวจสอบผ่านแหล่งให้ข้อมูลที่น่าเชื่อถือ เพื่อให้มั่นใจว่าผู้สมัครใช้บริการเป็นบุคคลเดียวกับหลักฐานแสดงตนนั้นจริง จึงจะสามารถทำธุรกรรมทางอิเล็กทรอนิกส์ได้ สามารถใช้การพิสูจน์ตัวตนในระดับความน่าเชื่อถือของไอเดนทิตี **อย่างน้อยระดับที่ ๒**

(๔) กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง จัดเป็นบริการที่มีความเสี่ยงสูง และต้องรู้จักตัวตนของผู้ใช้บริการ สามารถใช้การพิสูจน์ตัวตนในระดับความน่าเชื่อถือของไอเดนทิตี **อย่างน้อยระดับที่ ๓**

หมายเหตุ *กรณีที่ต้องมีการตรวจสอบหลักฐานแสดงตนกับแหล่งให้ข้อมูลที่น่าเชื่อถือมากกว่า ๑ แหล่งขึ้นไป ให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เช่น ศูนย์แลกเปลี่ยนข้อมูลกลาง โดยไม่ต้องร้องขอข้อมูลจากผู้สมัครใช้บริการเพิ่มเติม*

อนึ่ง หากบริการภาครัฐใดที่ต้องใช้ข้อมูลส่วนบุคคลในการพิสูจน์และยืนยันตัวตน ให้กำหนดระดับความน่าเชื่อถือของไอเดนทิตีขั้นต่ำที่ระดับ ๒ ซึ่งเทียบเท่ากับระดับความน่าเชื่อถือของไอเดนทิตีที่ระดับ ๒.๑ ของประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน

รายละเอียดแนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ ดังตารางที่ ๒

ตารางที่ ๒ แนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ	IAL1	การรวบรวมข้อมูลเพื่อระบุตัวตน	เจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตนของผู้สมัครใช้บริการหรือไม่ก็ได้	เจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตนของผู้สมัครใช้บริการผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดเพื่อแสดงตนหรือไม่ก็ได้	เจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตนของผู้สมัครใช้บริการผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดเพื่อแสดงตนหรือไม่ก็ได้
		การตรวจสอบหลักฐานแสดงตน	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP และเจ้าหน้าที่ดูรูปหลักฐานแสดงตนเพื่อตรวจสอบว่าเป็นของแท้	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP และเจ้าหน้าที่ดูรูปหลักฐานแสดงตน เพื่อตรวจสอบว่าเป็นของแท้

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
				- เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตนเพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตนเพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
		การตรวจสอบช่องทางการติดต่อ	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้ เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้ เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้ เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่
กลุ่มการให้บริการธุรกรรม	IAL2	การรวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ ต้องให้ข้อมูลเพื่อแสดงตน โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน เช่น ชื่อ ชื่อสกุล ที่อยู่ อีเมล หมายเลขโทรศัพท์เคลื่อนที่	ผู้สมัครใช้บริการ ต้องให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ ต้องให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน
		การตรวจสอบหลักฐานแสดงตน	IdP ต้องตรวจสอบข้อมูลหลักฐานแสดงตน ที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP ต้องตรวจสอบข้อมูลหลักฐานแสดงตน ที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP ต้องตรวจสอบข้อมูลหลักฐานแสดงตน ที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- เจ้าหน้าที่ใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนดของ IdP เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - IdP เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนดของ IdP เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	- เจ้าหน้าที่อาจถ่ายรูปและบันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าหน้าที่เปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้า	- ผู้สมัครใช้บริการถ่ายรูปตัวเองพร้อมหลักฐานแสดงตนผ่านแอปพลิเคชันของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าหน้าที่เปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison)	- ผู้สมัครใช้บริการถ่ายรูปตัวเองผ่านแอปพลิเคชัน เว็บไซต์หรือเทคโนโลยีที่กำหนดของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าหน้าที่เปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจาก

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			หรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	- กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	หลักฐานแสดงตน (physical comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)
		การตรวจสอบช่องทางการติดต่อ	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล
กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง	IAL3	การรวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ<u>ต้อง</u>ให้ข้อมูลเพื่อแสดงตน โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน		ผู้สมัครใช้บริการ<u>ต้อง</u>ให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน
		การตรวจสอบหลักฐานแสดงตน	IdP <u>ต้อง</u>ขอหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้		IdP <u>ต้อง</u>ขอหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป - เจ้าหน้าที่ดูหลักฐานแสดงตนและใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ หรือตรวจสอบแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่นเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับ		- ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป - เจ้าหน้าที่ดูหลักฐานแสดงตนและใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ หรือตรวจสอบแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่นเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			ข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง		ข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	- เจ้าหน้าที่บันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) เช่น ภาพใบหน้า ลายนิ้วมือ - ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)		- เจ้าหน้าที่บันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) เช่น ภาพใบหน้า ลายนิ้วมือ - ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)
		การตรวจสอบช่องทางการติดต่อ	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล		IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล

การยืนยันตัวตนทางดิจิทัล (Authentication)

๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล (Authentication Requirements)

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ ให้เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖] ข้อ ๒. ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level) โดยปัจจัยของการยืนยันตัวตน (authentication factor) มีรายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๔.๓.๑ สิ่งที่ใช้ยืนยันตัวตน (authenticator)

๓.๑ ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL)

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ ซึ่งการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๑ (AAL1)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นอย่างน้อย หรือหากต้องการความมั่นคงปลอดภัยที่สูงขึ้น สามารถยืนยันตัวตนแบบหลายปัจจัยได้ (multi-factor authentication) และต้องเป็นโพรโทคอลที่มีความปลอดภัย (secure authentication protocol) เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๒ (AAL2)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยที่แตกต่างกัน ซึ่งอาจเป็น (๑) สิ่งที่ใช้ยืนยันตัวตนหลายปัจจัย (multi-factor authenticator) เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซึ่งจะสร้างรหัสผ่านแบบใช้ครั้งเดียวหลังจากตรวจสอบลายนิ้วมือของผู้ใช้บริการ หรือ (๒) สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว (single-factor authenticator) อย่างน้อย ๒ สิ่งที่เป็นปัจจัยต่างกัน โดยที่ต้องเป็นรหัสผ่าน (something you know) ควบคู่กับการใช้ OTP ผ่านหมายเลขโทรศัพท์เคลื่อนที่ (something you have) โดยโพรโทคอลที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องเป็นโพรโทคอลที่มีความปลอดภัย เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๓ (AAL3)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยขึ้นไปที่แตกต่างกัน โดยมีปัจจัยหนึ่งเป็นกุญแจ (key) ที่ผ่านเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) ซึ่งผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองกุญแจนั้น และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตนดังกล่าวผ่านโพรโทคอลที่มีความปลอดภัยในการใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน และต้องมีการเข้ารหัสข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว (sensitive data) รวมถึงสิ่งที่ใช้ยืนยันตัวตนเพื่อป้องกันการปลอมแปลง เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

๓.๒ ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน (Authenticator and Verifier Requirements)

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖] ข้อ ๓. ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน

ทั้งนี้ การเปลี่ยนแปลงทางเทคโนโลยีหรือภัยคุกคาม อาจเกิดข้อจำกัดของสิ่งที่ใช้ยืนยันตัวตนที่ทำให้เสื่อมคุณภาพลง (restricted authenticator) โดยผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการ ดังนี้

(๑) เสนอทางเลือกของสิ่งที่ใช้ยืนยันตัวตนที่ยังไม่เสื่อมคุณภาพและสอดคล้องกับข้อกำหนดของระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๒) จัดทำเอกสารแจ้งข้อมูล (notice) ให้ผู้ใช้บริการทราบถึงความเสี่ยงด้านความมั่นคงปลอดภัยของสิ่งที่ใช้ยืนยันตัวตนที่เสื่อมคุณภาพ รวมถึงทางเลือกของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

(๓) ประเมินความเสี่ยงเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตนที่อาจเสื่อมคุณภาพลงของผู้ใช้บริการเพิ่มเติม

(๔) จัดทำแผนการบรรเทาความเสี่ยงสิ่งที่ใช้ยืนยันตัวตนที่อาจเสื่อมคุณภาพ

๓.๓ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Lifecycle Management)

การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ประกอบด้วยกระบวนการ ดังนี้

๓.๓.๑ การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (Authenticator Binding)

การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน คือ การสร้างความสัมพันธ์ระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการที่ออกโดยผู้พิสูจน์และยืนยันตัวตนในขั้นตอนของการลงทะเบียนเพื่อนำสิ่งที่ใช้ยืนยันตัวตนไปใช้ในการยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) ต้องเก็บรักษาข้อมูลที่เกี่ยวข้องกับสิ่งที่ใช้ยืนยันตัวตนทั้งหมดที่เป็นหรือมีความสัมพันธ์ในแต่ละไอเดนทิตีของผู้ใช้บริการ โดยอย่างน้อยต้องเก็บรักษาข้อมูลวันและเวลาที่สร้างความสัมพันธ์ระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตี และควรรวมถึงแหล่งของการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน เช่น IP address

(๒) ต้องเก็บรักษาข้อมูลเกี่ยวกับจำนวนครั้งของการยืนยันตัวตนผิดพลาดต่อเนื่อง เพื่อจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด

(๓) ต้องตรวจสอบชนิดของสิ่งที่ใช้ยืนยันตัวตนให้เป็นไปตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน เช่น หากใช้สิ่งที่ใช้ยืนยันตัวตนหลายปัจจัยต้องใช้วิธีการยืนยันตัวตนแบบหลายปัจจัยเช่นกัน

(๔) ต้องเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอย่างน้อย ๑ ปัจจัยและควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอย่างน้อย ๒ ปัจจัย โดยที่ปัจจัยใดปัจจัยหนึ่งเป็นสิ่งที่ผู้ใช้บริการมี (something you have) เช่น โทเค็น (token) เพื่อให้สามารถกู้คืนได้ กรณีที่เกิดการสูญหาย ถูกโจรกรรม เช่น ผู้ใช้บริการใช้อุปกรณ์ OTP ปัจจัยเดียวแล้วเกิดการเสียหาย จะใช้รหัสลับจดจำในการกู้คืน

(๕) ในกรณีที่การลงทะเบียนและเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนไม่สมบูรณ์ต้องใช้รหัสผ่านแบบชั่วคราว ทั้งนี้การใช้รหัสผ่านแบบชั่วคราวต้องไม่นำมาใช้ซ้ำ โดยจัดส่งไปยังหมายเลขโทรศัพท์เคลื่อนที่หรืออีเมลของผู้สมัครใช้บริการ หรือใช้ข้อมูลชีวมิติที่ได้จัดเก็บไว้ตอนลงทะเบียนแบบพบเห็นต่อหน้าในการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

๓.๓.๒ การสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน (Loss, Theft and Damage)

สิ่งที่ใช้ยืนยันตัวตนที่สูญหาย ถูกโจรกรรม หรือเสียหาย ถือว่าเป็นสิ่งที่ใช้ยืนยันตัวตนที่เสี่ยงต่อการใช้งานโดยผู้ไม่ประสงค์ดีในการนำสิ่งที่ใช้ยืนยันตัวตนไปใช้โดยไม่มีสิทธิ ดังนั้น ผู้พิสูจน์และยืนยันตัวตน จึงควรให้ความสำคัญกับแนวปฏิบัติในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม และเสียหาย

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) ต้องจัดให้มีช่องทางสำหรับรายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน

(๒) ควรจัดให้มีวิธีการยืนยันตัวตนสำรองหรือวิธีการอื่น ๆ ที่ใช้ตรวจสอบว่ารายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน มาจากผู้ใช้บริการที่กล่าวอ้างจริง

(๓) ต้องระงับการใช้งาน เพิกถอน หรือทำลายสิ่งที่ใช้ยืนยันตัวตนทันที หลังจากตรวจพบว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม หรือเสียหาย

(๔) หลังจากสิ่งที่ใช้ยืนยันตัวตนถูกระงับการใช้งาน อาจมีการกำหนดระยะเวลาของการเปิดใช้งานใหม่อีกครั้ง หากเกินจากระยะเวลาที่กำหนดจะไม่สามารถกลับมาใช้งานได้อีก

(๕) ต้องดำเนินการพิสูจน์ตัวตนผู้ใช้บริการใหม่อีกครั้ง แต่ไม่จำต้องพิสูจน์ตัวตนใหม่ทั้งหมด ทั้งนี้ อาจตรวจสอบความสัมพันธ์ระหว่างตัวตนผู้ใช้บริการกับข้อมูลและหลักฐานแสดงตนที่ได้จัดเก็บไว้ในการลงทะเบียนและพิสูจน์ตัวตนไว้ก่อนหน้าด้วยวิธีการที่เหมาะสม

๓.๓.๓ การหมดอายุ (Expiration)

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุต้องไม่สามารถใช้ยืนยันตัวตนได้

(๒) เมื่อมีการยืนยันตัวตนโดยใช้สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุ ควรแจ้งให้ผู้ใช้บริการทราบว่าการยืนยันตัวตนไม่สำเร็จเนื่องจากสิ่งที่ใช้ยืนยันตัวตนหมดอายุ

(๓) ควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนใหม่หรือต่ออายุการใช้งานสิ่งที่ใช้ยืนยันตัวตนในระยะเวลาที่เหมาะสมก่อนที่สิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการจะหมดอายุ

(๔) ต้องเพิกถอนหรือทำลายสิ่งที่ใช้ยืนยันตัวตนเดิม เมื่อผู้ใช้บริการได้รับและใช้สิ่งที่ใช้ยืนยันตัวตนใหม่

๓.๓.๔ การเพิกถอน (Revocation)

การเพิกถอนสิ่งที่ใช้ยืนยันตัวตน คือ การยุติความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตน ต้องเพิกถอนสิ่งที่ใช้ยืนยันตัวตนทันที เมื่อมีกรณีใดกรณีหนึ่ง ดังนี้

(๑) ไอเดนทิตีถูกเพิกถอน เช่น ผู้ใช้บริการเสียชีวิต ผู้ใช้บริการถูกตรวจพบว่ามีการหลอกลวงหรือปลอมแปลง หรือไม่แสดงตัวตนจริง

(๒) ผู้ใช้บริการต้องการเพิกถอนสิ่งที่ใช้ยืนยันตัวตนหรือยกเลิกการใช้บริการกับผู้พิสูจน์และยืนยันตัวตน

(๓) ในกรณีที่ตรวจพบในภายหลังว่าผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเกณฑ์ที่ผู้พิสูจน์และยืนยันตัวตนกำหนด

๓.๔ การบริหารจัดการเซสชัน (Session Management)

การกำหนดเซสชัน อาจเริ่มตั้งแต่การยืนยันตัวตนไปจนถึงการสิ้นสุดการใช้งาน ทั้งนี้ การยกเลิกเซสชัน อาจเกิดขึ้นได้ เช่น การไม่มีกิจกรรมใด ๆ เกิดขึ้นในระยะเวลาที่กำหนด หรือถูกยกเลิกโดยผู้ใช้บริการ หากต้องการใช้บริการต่อจากเซสชันเดิมที่ถูกยกเลิกแล้ว ให้ผู้ใช้บริการยืนยันตัวตนซ้ำอีกครั้งเพื่อเข้าใช้งาน

๓.๔.๑ การเชื่อมโยงเซสชัน (Session Binding)

เซสชันจะเกิดขึ้นระหว่างแอปพลิเคชันของผู้ใช้บริการ (session subject) เช่น เว็บไซต์ ระบบปฏิบัติการ กับผู้ให้บริการภาครัฐหรือผู้พิสูจน์และยืนยันตัวตน (session host) ที่เข้าถึงโดยผู้ใช้บริการหลังจากยืนยันตัวตนสำเร็จ

ความลับของเซสชัน (session secret) ต้องใช้ร่วมกันระหว่างแอปพลิเคชันของผู้ใช้บริการกับบริการที่เข้าถึงเพื่อให้สามารถใช้งานได้อย่างต่อเนื่องจนถึงสิ้นสุดการใช้งาน โดยความลับของเซสชันจะต้องมีกลไกในการเข้ารหัส (cryptographic mechanism) ทั้งนี้ การเชื่อมโยงเซสชันต้องสอดคล้องกับคุณสมบัติตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนด้วย ความลับในการเชื่อมโยงเซสชัน มีดังนี้

(๑) ต้องสร้างขึ้นทันทีโดย session host หลังจากการยืนยันตัวตนสำเร็จ

(๒) ต้องสร้างขึ้นโดยวิธีการสุ่ม และประกอบด้วยอย่างน้อย ๖๔ บิต

(๓) ต้องลบหรือทำให้ใช้งานไม่ได้โดย session subject หลังจากที่ผู้ใช้บริการออกจากระบบ

(๔) ควรลบการเชื่อมโยงเซสชัน เมื่อผู้ใช้บริการออกจากระบบหรือเมื่อความลับหมดอายุการใช้งาน

(๕) ไม่ควรจัดเก็บเซสชันไว้ในสถานที่ที่ไม่ปลอดภัย เช่น HTML5 ซึ่งอาจเสี่ยงต่อการโจมตีแบบ cross-site scripting (XSS)

(๖) ต้องส่งและรับเซสชันจากอุปกรณ์ผ่านช่องทางที่มีความปลอดภัย

(๗) ต้องตั้งเวลาหมดอายุ ไม่ให้ใช้งานได้ ดังนี้

(๗.๑) ๓๐ วัน สำหรับ AAL1

(๗.๒) ๑๒ ชั่วโมง หรือ ๓๐ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL2

(๗.๓) ๑๒ ชั่วโมง หรือ ๑๕ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL3

(๘) ต้องไม่สามารถใช้งานผ่านช่องทางการสื่อสารที่ไม่ปลอดภัย และเมื่อยืนยันตัวตนสำเร็จต้องไม่ลดระดับไปยังช่องทางการสื่อสารที่ไม่ปลอดภัย เช่น จาก HTTPS เป็น HTTP

๓.๔.๑.๑ เบราว์เซอร์คุกกี้ (Browser Cookies)

เบราว์เซอร์คุกกี้เป็นกลไกที่ใช้สำหรับสร้างเซสชัน และติดตามผู้ใช้บริการขณะที่เข้าใช้บริการ ควรกำหนดดังนี้

(๑) ต้องกำหนดให้มีการเข้าถึงคุกกี้ได้เฉพาะการเชื่อมต่อที่ใช้งาน HTTPS เท่านั้น

(๒) ต้องระบุ hostname และ path ที่อนุญาตให้ใช้คุกกี้น้อยที่สุดเท่าที่จำเป็น

(๓) ควรกำหนดให้ JavaScript ไม่สามารถเข้าถึงคุกกี้ได้ โดยการกำหนด flag HttpOnly ให้กับคุกกี้

(๔) ควรกำหนดระยะเวลาหมดอายุของคุกกี้

๓.๔.๑.๒ แอกเซสโทเค็น (Access Token)

แอกเซสโทเค็นใช้สำหรับอนุญาตให้แอปพลิเคชันเข้าถึงบริการภาครัฐในฐานะของผู้ใช้บริการหลังจากการยืนยันตัวตนสำเร็จ โดยผู้ให้บริการภาครัฐต้องไม่ถือว่าการแสดง OAuth access token เป็นการยืนยันตัวตนตามหลักการของดิจิทัลไอดี ซึ่งอาจใช้องค์ประกอบอื่น ๆ เพิ่มเติมด้วย เนื่องจาก OAuth access token และ refresh token ที่เกี่ยวข้อง อาจคงสถานะการใช้งานได้หลังจากการสิ้นสุดเซสชันและผู้ใช้บริการได้ออกจากแอปพลิเคชันไปแล้ว

๓.๔.๑.๓ การระบุอุปกรณ์ (Device Identification)

วิธีการระบุอุปกรณ์ที่มีความปลอดภัย เช่น การใช้โพรโทคอล TLS หรือการเชื่อมโยงโทเค็น (token binding) หรือวิธีการอื่น ๆ อาจนำมาใช้สร้างเซสชันระหว่างผู้ใช้บริการกับบริการภาครัฐได้

๓.๔.๒ การยืนยันตัวตนซ้ำ (Reauthentication)

ความต่อเนื่องของเซสชันต้องขึ้นอยู่กับความลับของเซสชันที่ครอบครองในช่วงเวลาของการยืนยันตัวตนที่ออกโดยผู้พิสูจน์และยืนยันตัวตน และอาจมีการ refresh session

ความลับของเซสชันต้องไม่คงอยู่ถาวรและต้องไม่เก็บไว้หากมีการเริ่มใช้งาน (restart) แอปพลิเคชันใหม่ หรือรีบูต (reboot) เครื่องที่ให้บริการ

การยืนยันตัวตนซ้ำตามช่วงเวลาที่กำหนดของแต่ละระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ต้องเกิดขึ้นเพื่อยืนยันว่าผู้ใช้บริการยังคงมีสถานะใช้งานอยู่ ก่อนที่เซสชัน

จะสิ้นสุดเนื่องจากหมดเวลาหรือด้วยเหตุผลอื่น ๆ ผู้ใช้บริการต้องยืนยันตัวตนซ้ำเพื่อต่ออายุการใช้งานเซสชันโดยมีวิธีการ ดังนี้

(๑) ระดับ AAL1 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

(๒) ระดับ AAL2 : ยืนยันตัวตนโดยใช้รหัสลับจดจำหรือชีวมิติ

(๓) ระดับ AAL3 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด

เมื่อถึงเวลาที่กำหนดไว้ เซสชันควรถูกทำให้สิ้นสุดลง (terminated) เช่น การออกจากระบบ ทั้งนี้ เมื่อเซสชันถูกทำให้สิ้นสุดลงแล้ว ผู้ใช้บริการจะต้องยืนยันตัวตนใหม่อีกครั้งโดยต้องมีการสร้างเซสชันใหม่ขึ้นมา

๓.๕ ภัยคุกคาม (Threats and Security Considerations)

นอกจากนี้ ในกระบวนการยืนยันตัวตนต้องคำนึงถึงภัยคุกคามที่อาจจะก่อให้เกิดความเสียหายแก่ระบบงานและข้อมูลต่าง ๆ ขึ้นได้ ดังนี้

ตารางที่ ๓ ภัยคุกคามและการบรรเทาภัยคุกคามที่อาจเกิดขึ้นในขั้นตอนการยืนยันตัวตน

ภัยคุกคาม	รายละเอียด	ตัวอย่าง	การบรรเทาภัยคุกคามที่อาจเกิดขึ้น
การเดาออนไลน์ (online guessing)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีพยายามเข้าระบบ (login) ซ้ำ ๆ โดยทดลองเดาผลลัพธ์หรือค่าต่าง ๆ ที่จะสามารถผ่านเข้าไปยังระบบได้	การพยายามเข้าเว็บไซต์โดยลักลอบใช้ชื่อผู้ใช้งาน (username) และทดลองใช้รหัสผ่าน (password) ที่ผู้ใช้บริการอาจใช้บ่อย ๆ	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีล่วงรู้หรือคาดเดาข้อมูลเฉพาะของผู้ใช้บริการที่ใช้เป็นข้อมูลลับในการยืนยันตัวตน โดย IdP ควรคำนึงถึงระดับความยากง่ายของการสร้างข้อมูลลับ ความปลอดภัยของข้อมูลที่รับส่งผ่านช่องทางการยืนยันตัวตน และวิธีการบริหารจัดการอื่น ๆ เช่น การใช้รหัสผ่านที่คาดเดายาก และจำกัดจำนวนครั้งของความพยายามในการยืนยันตัวตนที่ไม่สำเร็จ หากครบจำนวนแล้วต้องกำหนดระยะเวลาที่สามารถเข้าสู่ระบบได้ใหม่ในครั้งถัดไป
การส่งข้อมูลซ้ำ (replay attack)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีสามารถนำข้อมูลที่เคยดักจับได้กลับมาใช้ยืนยันตัวตนเพื่อเข้าระบบเสมือนเป็นผู้ใช้บริการ	ผู้ไม่ประสงค์ดีอาจดักจับรหัสผ่านจากผู้ใช้บริการในขณะยืนยันตัวตน และนำรหัสผ่านนั้นมาเข้าระบบในภายหลัง	ใช้ช่องทางการสื่อสารที่มีการตรวจสอบความเป็นปัจจุบัน หรือมีการจำกัดเวลาของการใช้งานที่สอดคล้องกับช่วงเวลาในการยืนยันตัวตนในปัจจุบัน
การขโมยเซสชัน (session hijack)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมเซสชัน ซึ่งอาจจะเป็นการแฝงตัวในการสื่อสารที่แลกเปลี่ยนข้อมูลการยืนยันตัวตนระหว่างผู้ใช้บริการและ IdP เพื่อเข้าควบคุมการสื่อสารนั้นไว้	ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมการสื่อสารที่แลกเปลี่ยนข้อมูลการยืนยันตัวตน แล้วดักจับข้อมูลหรือคาดเดาค่า (value) ของคุกกี้ที่ใช้ในการยืนยันตัวตน (authentication cookies) เพื่อระบุ HTTP requests ของผู้ใช้บริการ	ใช้ช่องทางสื่อสารในการยืนยันตัวตนระหว่างผู้ใช้บริการและ IdP ที่มีการควบคุมการรับส่งข้อมูลต่อช่วงเวลา (per-session data transfer protocol)

ภัยคุกคาม	รายละเอียด	ตัวอย่าง	การบรรเทาภัยคุกคามที่อาจเกิดขึ้น
การแอบดักจับข้อมูล (eavesdropping)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีลักลอบดักจับข้อมูลจากช่องทางการสื่อสาร เพื่อนำข้อมูลที่ได้ไปใช้ปลอมแปลงเป็นผู้ใช้บริการในการยืนยันตัวตนเข้าระบบ	แอบส่องรหัสลับจดจำเมื่อผู้ใช้งานพิมพ์รหัสลงบนแป้นพิมพ์ หรือใช้ซอฟต์แวร์ดักจับข้อมูลที่ได้มีการบันทึกการพิมพ์รหัสลงบนแป้นพิมพ์ (keystroke)	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีล่วงรู้ข้อมูลเฉพาะของผู้ใช้บริการ ที่ใช้เป็นข้อมูลลับในการยืนยันตัวตนโดยใช้ช่องทางการสื่อสารที่ป้องกันการดักจับข้อมูล รวมถึงควรมีมาตรการมิให้บุคคลอื่นที่ทำการดักจับข้อมูลสามารถนำข้อมูลไปใช้ได้ เช่น transport layer security (TLS) protocol
การหลอกลวง (phishing)	เป็นวิธีการที่ผู้ใช้บริการถูกล่อลวงโดยผู้ไม่ประสงค์ดี เพื่อให้เปิดเผยข้อมูลลับ ข้อมูลส่วนตัว หรือข้อมูลที่ใช้ในการยืนยันตัวตน โดยผู้ไม่ประสงค์ดีจะนำข้อมูลต่าง ๆ ที่ได้ไปปลอมตัวเป็นผู้ใช้บริการ เพื่อยืนยันตัวตนเข้าใช้บริการภาครัฐ	การส่งอีเมลเพื่อล่อลวงให้ผู้ใช้บริการเข้าไปยังเว็บไซต์ที่ผู้ไม่ประสงค์ดีทำปลอมขึ้นมา โดยทำให้ผู้ใช้บริการคิดว่าเป็นเว็บไซต์จริง และล่อลวงให้ใส่ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าระบบ เช่น เว็บไซต์ของ IdP ที่ผู้ใช้บริการมีบัญชี (account) อยู่	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถล่วงรู้หรือเรียนรู้ข้อมูลและพฤติกรรมส่วนตัวของผู้ใช้บริการ รวมถึงสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ
การลักลอบเป็นคนกลาง (man-in-the-middle)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีแฝงตัวอยู่ในช่องทางการสื่อสารเพื่อลักลอบ ขัดขวาง แก้ไข หรือใช้เนื้อหาข้อมูลที่แลกเปลี่ยนกันในการยืนยันตัวตนระหว่างผู้ใช้บริการและ IdP เพื่อให้ผู้ไม่ประสงค์ดีสามารถเข้าระบบได้ โดยปกติแล้วผู้ไม่ประสงค์ดีจะปลอมตัวเป็น IdP เพื่อหลอกผู้ใช้บริการ และในทำนองเดียวกันก็สามารถปลอมตัวเป็นผู้ใช้บริการเพื่อหลอก IdP ตัวตนได้เช่นกัน	ถ้าผู้ใช้บริการต้องการส่งข้อมูลไปยัง IdP โดยมีการเข้ารหัสข้อมูลด้วยกุญแจสาธารณะของ IdP ในช่องทางการสื่อสาร ผู้ไม่ประสงค์ดีจะทำการสับเปลี่ยนกุญแจสาธารณะโดยส่งกุญแจสาธารณะของผู้ไม่ประสงค์ดีไปให้ผู้ใช้บริการและล่อลวงให้เข้ารหัสด้วยกุญแจสาธารณะนั้นแทน ซึ่งผู้ไม่ประสงค์ดีจะสามารถถอดรหัสข้อมูลนั้นได้ด้วยกุญแจส่วนตัวของผู้ไม่ประสงค์ดี	ตรวจสอบกระบวนการยืนยันตัวตน ให้แน่ใจว่าข้อมูลที่ถูกส่งระหว่างกันไม่สามารถดักจับได้ หากมีการส่งความลับ (secret) หรือข้อมูลส่วนตัวผ่านทางอินเทอร์เน็ต ต้องทำการเข้ารหัสก่อนทุกครั้ง ควรใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) ในการยืนยันตัวตนระหว่างฝั่งของผู้ใช้บริการและฝั่งของ IdP หรือใช้ช่องทางที่อนุญาตให้ผู้ใช้บริการเปิดเผยความลับไปยัง IdP ตัวจริงเท่านั้น

๓.๖ ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล (Minimum Requirement of Authentication)

เมื่อผู้ใช้บริการลงทะเบียนและพิสูจน์ตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนเรียบร้อยแล้ว หากผู้ใช้บริการต้องการเข้าใช้บริการออนไลน์กับผู้ให้บริการภาครัฐและผู้ให้บริการภาครัฐต้องการทราบว่าผู้ใช้บริการเป็นผู้ใด

สำหรับผู้ใช้บริการที่เคยลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนที่ผู้ให้บริการภาครัฐเชื่อถือ ผู้ให้บริการภาครัฐจะนำผู้ใช้บริการไปยังหน้าต่างยืนยันตัวตนของผู้พิสูจน์และยืนยันตัวตนนั้น ผู้ใช้บริการต้องยืนยันตัวตนด้วยการพิสูจน์ให้เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ผู้พิสูจน์และยืนยันตัวตนกำหนด เมื่อตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตนเรียบร้อยแล้ว ผู้พิสูจน์และยืนยันตัวตนจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐ เพื่อให้ผู้ให้บริการภาครัฐนำไปใช้พิจารณาอนุญาตเข้าใช้บริการภาครัฐต่อไป

ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล จำแนกตามกลุ่มการให้บริการภาครัฐ ดังนี้

(๑) กลุ่มการให้บริการข้อมูลพื้นฐาน จัดเป็นบริการที่ไม่มีความเสี่ยงหรือมีความเสี่ยงต่ำ จึง**ไม่จำเป็นต้องใช้ดิจิทัลไอดี**

(๒) กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ จัดเป็นบริการที่มีความเสี่ยงต่ำ สามารถใช้การยืนยันตัวตนในระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน **อย่างน้อยระดับที่ ๑**

(๓) กลุ่มการให้บริการธุรกรรม จัดเป็นบริการที่มีความเสี่ยงปานกลางถึงสูง โดยจำนวนและประเภทของปัจจัยของการยืนยันตัวตนมีผลกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นบุคคลที่ได้ลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนจริง สามารถใช้การยืนยันตัวตนในระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน **อย่างน้อยระดับที่ ๒**

(๔) กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง จัดเป็นบริการที่มีความเสี่ยงสูง สามารถใช้การยืนยันตัวตนในระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน **อย่างน้อยระดับที่ ๒**

รายละเอียดแนวทางการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของกลุ่มการให้บริการภาครัฐ ดังตารางที่ ๔

ตารางที่ ๔ แนวทางการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของกลุ่มการให้บริการภาครัฐ

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ	AAL1	ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ - รหัสลับจดจำ (memorized secret) - อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) - อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) - ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) - อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device) - สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL๒ และ AAL๓
		การยืนยันตัวตนซ้ำ	อย่างน้อยทุก ๓๐ วัน
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
- **กลุ่มการให้บริการธุรกรรม** - **กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง**	AAL2	ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ - อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device) - ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software) - รหัสลับจดจำ (memorized secret) ร่วมกับอุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) - รหัสลับจดจำ (memorized secret) ร่วมกับอุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) - รหัสลับจดจำ (memorized secret) ร่วมกับซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) - รหัสลับจดจำ (memorized secret) ร่วมกับอุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device) - ชีวมิติ (biometric) ร่วมกับชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกข้างต้น - สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL๓
		การยืนยันตัวตนซ้ำ	- อย่างน้อยทุก ๑๒ ชั่วโมง **หรือ** - ๓๐ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น ผู้ใช้บริการอาจยืนยันตัวตนโดยใช้ ๑ ปัจจัย (รหัสลับจดจำหรือชีวมิติ)
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น
	AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ - อุปกรณ์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic device) - อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device) ร่วมกับ รหัสลับจดจำ (memorized secret) - อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device) ร่วมกับอุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device) - อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device) ร่วมกับซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) - อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) ร่วมกับซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software) - อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) ร่วมกับซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) และรหัสลับจดจำ (memorized secret)

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
		การยืนยันตัวตนซ้ำ	- อย่างน้อยทุก ๑๒ ชั่วโมง **หรือ** - ๑๕ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น ผู้ใช้บริการต้องยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	จำเป็น

๔. การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล (Privacy Considerations)

การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล ควรพิจารณาดังนี้

๔.๑ การจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization)

ตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๒ กำหนดให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยต้องมีแนวทางในการดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็นทั้งในแง่ของประเภทข้อมูลและระยะเวลาการจัดเก็บข้อมูล ซึ่งการจัดเก็บข้อมูลเท่าที่จำเป็นจะเป็นการลดความเสี่ยงที่อาจเกิดขึ้นได้จากการใช้งานหรือเข้าถึงโดยไม่ได้รับอนุญาต

ทั้งนี้ ในการจัดเก็บข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงการดำเนินการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ

๔.๒ เอกสารแจ้งข้อมูลและเอกสารแสดงความยินยอม (Privacy Notice and Consent)

ตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๑๙ ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว

ทั้งนี้ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลต้องเป็นไปตามแบบและข้อความตามที่กฎหมายกำหนด ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการนั้น ๆ เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบ

ในกรณีถอนความยินยอมผู้พิสูจน์และยืนยันตัวตนต้องแจ้งส่งผลกระทบจากการถอนความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ ทั้งนี้ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กฎหมายกำหนด จะไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล และผู้พิสูจน์และยืนยันตัวตนไม่สามารถเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้

๔.๓ การคุ้มครองความเป็นส่วนบุคคล (Privacy Control)

ผู้พิสูจน์และยืนยันตัวตนควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม โดยครอบคลุมถึงการแจ้งเตือน การแก้ไข หรือการพิจารณาอื่น ๆ ที่สำคัญ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมถึงการขอความยินยอมต้องทำเป็นลายลักษณ์อักษรที่ชัดเจน และทำผ่านระบบอิเล็กทรอนิกส์ได้

๔.๔ การใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น (Use Limitation)

การใช้และประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์และการแสดงความยินยอมของเจ้าของข้อมูลส่วนบุคคลในเรื่องนั้น ๆ หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับกรณีใดบ้าง ในกรณีที่ไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล มีดังนี้

(๑) เพื่อจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษา วิจัย หรือสถิติ ที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เพื่อปฏิบัติตามหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เพื่อปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนควรประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล และควรวัดผลการบริหารจัดการให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ไม่ให้สูงเกินจากที่กำหนดไว้ภายใต้บริการนั้น

๔.๕ การแก้ไขข้อมูลส่วนบุคคล (Redress)

ผู้พิสูจน์และยืนยันตัวตนต้องจัดให้มีกลไกสำหรับการแก้ไขข้อมูลตามข้อร้องเรียนหรือปัญหาของผู้สมัครใช้บริการที่เกิดขึ้นจากการพิสูจน์ตัวตน โดยกลไกดังกล่าวต้องให้ผู้สมัครใช้บริการค้นหาและใช้งานได้ง่าย ทั้งนี้ควรจัดให้มีวิธีการอื่น ๆ เช่น วิธีการแบบพบเห็นต่อหน้า เพื่อรองรับในกรณีที่ผู้สมัครใช้บริการไม่สามารถแก้ไขข้อมูลได้ด้วยวิธีการแบบออนไลน์

๔.๖ การประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Risk Assessment)

ผู้พิสูจน์และยืนยันตัวตน ควรพิจารณาดังนี้

(๑) โอกาสที่จะเกิดการดำเนินงานที่สร้างหรือก่อให้เกิดปัญหาต่อผู้สมัครใช้บริการหรือผู้ใช้บริการในระบบ เช่น ขั้นตอนการตรวจสอบหรือการจัดเก็บบันทึกข้อมูลส่วนบุคคลอาจทำให้เกิดการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

(๒) ผลกระทบเมื่อเกิดปัญหาขึ้น

ผู้พิสูจน์และยืนยันตัวตนควรมีแนวทางในการตอบสนองต่อความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการยอมรับความเสี่ยง การบรรเทาความเสี่ยง และการแบ่งปันความเสี่ยง ทั้งนี้ การให้ความยินยอมของผู้ใช้บริการถือเป็นรูปแบบหนึ่งของการแบ่งปันความเสี่ยง ซึ่งใช้ได้เฉพาะกับผู้ใช้บริการที่ยอมรับข้อตกลงและเงื่อนไขการให้บริการที่เหมาะสมเพียงพอที่จะแบ่งปันความเสี่ยงได้

๔.๗ การดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Compliance)

ผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงการดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ เช่น กฎหมาย ข้อกำหนด ข้อตกลง นโยบาย แนวปฏิบัติ เพื่อที่จะประเมินและบรรเทาความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการให้คำแนะนำกับหน่วยงานที่เกี่ยวข้องเพื่อปฏิบัติ

๕. แนวทางการนำไปใช้ (Usability Considerations)

ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสามารถกำหนดข้อตกลงร่วมกันในการพิสูจน์และยืนยันตัวตนทางดิจิทัลระหว่างผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ ดังนี้

๕.๑ สำหรับผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP)

๕.๑.๑ กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้สอดคล้องกับระดับความน่าเชื่อถือ

ต้องกำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้สอดคล้องกับระดับความน่าเชื่อถือ โดยจัดให้มีทรัพยากรที่เพียงพอ เหมาะสม มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัย เช่น กระบวนการ ระบบ เทคโนโลยี บุคลากร สถานที่ รายละเอียดตามมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้

๕.๑.๒ กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร

ต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่ที่ได้รับการฝึกอบรมหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

๕.๑.๓ ดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐต้องดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล รายละเอียดตามข้อ ๒. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล ดังนี้

(๑) รวบรวมข้อมูลเพื่อระบุตัวตน

(๒) ตรวจสอบหลักฐานแสดงตน

(๓) ตรวจสอบตัวบุคคล

ทั้งนี้ หากผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนให้ดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๕.๑.๔ ดำเนินการตามข้อกำหนดการยืนยันตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

ต้องดำเนินการตามข้อกำหนดของการยืนยันตัวตนทางดิจิทัล รายละเอียดตามข้อ ๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล

ทั้งนี้ต้องพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคล รายละเอียดตามข้อ ๔.

๕.๑.๕ ต้องจัดให้มีการขอความยินยอมของผู้สมัครใช้บริการ

โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย

๕.๑.๖ ต้องจัดให้มีการแสดงตนและรวบรวมข้อมูลเพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการ

เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

๕.๑.๗ ต้องเก็บรักษาข้อมูลและหลักฐานแสดงตน

รวมถึงภาพและเสียง (ถ้ามี) และการบันทึกเหตุการณ์และรายละเอียดการทำธุรกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยระยะเวลาการเก็บรักษาและการบันทึกดังกล่าวให้เป็นไปตามกฎหมาย ข้อบังคับ หรือแนวนโยบายที่เกี่ยวข้อง

๕.๑.๘ ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๕.๑.๙ ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

๕.๒ สำหรับผู้ให้บริการภาครัฐ

การเลือกใช้รูปแบบ วิธีการ รวมถึงระดับความน่าเชื่อถือที่เหมาะสมกับบริการภาครัฐนั้น มีความสำคัญอย่างยิ่ง ดังนั้นการออกแบบและการนำไปใช้ ต้องคำนึงถึงกระบวนการ [๗] ดังนี้

๕.๒.๑ กำหนดความต้องการและระบบของหน่วยงานของรัฐที่ต้องการใช้ดิจิทัลไอดี

ต้องกำหนดความต้องการและระบบของบริการภาครัฐของหน่วยงานของตนที่ต้องการใช้ดิจิทัลไอดี ทั้งนี้ ผลลัพธ์ที่ได้จะนำไปใช้ในการวิเคราะห์และประเมินความเสี่ยง โดยพิจารณาดังนี้

(๑) กำหนดบริการภาครัฐอย่างชัดเจนว่ามีบริการใดบ้างที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในการให้บริการ
(๒) กำหนดบริการภาครัฐอย่างชัดเจนว่าจำเป็นต้องลงทะเบียนและพิสูจน์ตัวตนหรือไม่
(๓) กำหนดผู้เกี่ยวข้อง บทบาท และหน้าที่
(๔) กำหนดช่องทางดิจิทัลที่ใช้ในการรับส่งข้อมูล เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่

๕.๒.๒ ประเมินความเสี่ยง

ต้องพิจารณาถึงผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์และยืนยันตัวตนผิดพลาด และควรมุ่งเน้นที่กระบวนการธุรกรรมออนไลน์เป็นหลัก รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๖.๓ ความเสี่ยงและผลกระทบ

๕.๒.๓ กำหนดระดับความน่าเชื่อถือ

ต้องนำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตีเมื่อเกิดข้อผิดพลาดในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลจากข้อ ๕.๒.๒ มาใช้พิจารณาระดับความน่าเชื่อถือของไอเดนทิตี รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๗. การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

และต้องนำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนเมื่อเกิดข้อผิดพลาดในการยืนยันตัวตนทางดิจิทัลจากข้อ ๕.๒.๒ มาใช้พิจารณาระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๘. การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๕.๒.๔ เลือกรูปแบบ และวิธีการลงทะเบียน พิสูจน์ตัวตน และยืนยันตัวตนทางดิจิทัล

พิจารณาจัดรูปแบบการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยผู้พิสูจน์และยืนยันตัวตนจะเป็นผู้รับผิดชอบดูแลเกี่ยวกับการรับลงทะเบียน การพิสูจน์ตัวตน และบริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยต้องมีการรวบรวมข้อมูลเพื่อระบุตัวตน การตรวจสอบหลักฐานแสดงตน การตรวจสอบตัวบุคคล หรือการตรวจสอบช่องทางการติดต่อ ตามแต่ละระดับความน่าเชื่อถือเพื่อกำหนดวิธีการลงทะเบียน รายละเอียดตามข้อ ๒. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน

ทางดิจิทัล รวมถึงเลือกปัจจัยและชนิดของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสม รายละเอียดตามข้อ ๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล

๕.๒.๕ ทบทวนความถูกต้องเหมาะสม

ต้องทบทวนถึงองค์ประกอบและความพร้อมทั้งหมดก่อนดำเนินการในกระบวนการพิสูจน์และยืนยันตัวตน นอกจากนี้ควรจะพิจารณาในเรื่องของค่าใช้จ่ายและผลประโยชน์ก่อนตัดสินใจดำเนินการต่าง ๆ รวมถึงควรประเมินระบบและเทคโนโลยีที่ใช้ในการพิสูจน์และยืนยันตัวตนเป็นประจำ

๕.๓ สำหรับแหล่งให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS)

๕.๓.๑ ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการ

เมื่อผู้สมัครใช้บริการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล แหล่งให้ข้อมูลที่น่าเชื่อถือจะตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

ทั้งนี้ หากบริการภาครัฐใดที่ต้องใช้ข้อมูลส่วนบุคคลในการพิสูจน์และยืนยันตัวตนทางดิจิทัล ให้กำหนดระดับความน่าเชื่อถือของไอเดนทิตีขั้นต่ำที่ระดับ ๒ ซึ่งเทียบเท่ากับระดับความน่าเชื่อถือของไอเดนทิตีที่ระดับ ๒.๑ ของประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน เมื่อครบระยะเวลาดังกล่าว

บรรณานุกรม

[๑] National Institute of Standards and Technology. (2017). *NIST Special Publication 800-63-3– Digital Identity Guidelines*. US Department of Commerce.

[๒] National Institute of Standards and Technology. (2017). *NIST Special Publication 800-63A– Digital Identity Guidelines – Enrollment and Identity Proofing*. US Department of Commerce.

[๓] National Institute of Standards and Technology. (2017). *NIST Special Publication 800-63B– Digital Identity Guidelines – Authentication and Lifecycle Management*. US Department of Commerce.

[๔] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๕] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๖] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

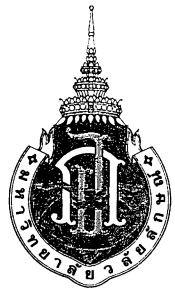
[๗] Department of Finance and Deregulation. (2009). *The National e-Authentication Framework*. Australian Government Information Management Office.

[๘] Department of Economic and Social Affairs. (2012). *United Nations E-Government Survey ๒๐๑๒.* United Nations, New York.

[๙] ธนาคารแห่งประเทศไทย. (๒๕๖๒). *หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน*. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ ประกาศ ณ วันที่ ๒๓ สิงหาคม ๒๕๖๒ คัดจากราชกิจจานุเบกษา เล่มที่ ๑๓๖ ตอนพิเศษ ๒๑๙ ง วันที่ ๒ กันยายน ๒๕๖๒.

[๑๐] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

ภาคผนวก 6 ข้อบังคับมหาวิทยาลัยมหาวิทยาลัยวลัยลักษณ์
ว่าด้วยประมวลจริยธรรมและธรรมาภิบาลนายกสภา มหาวิทยาลัย กรรมการสภามหาวิทยาลัย
ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕



ข้อบังคับมหาวิทยาลัยวลัยลักษณ์
ว่าด้วยประมวลจริยธรรมและธรรมาภิบาลนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย
ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัยวลัยลักษณ์
พ.ศ. ๒๕๖๕

.....

ตามที่พระราชบัญญัติการอุดมศึกษา พ.ศ. ๒๕๖๒ มาตรา ๒๐ กำหนดให้สภาสถาบันอุดมศึกษาต้องจัดให้มีประมวลจริยธรรมของนายกสภาสถาบันอุดมศึกษา กรรมการสภาสถาบันอุดมศึกษา ผู้บริหาร บุคลากรของสถาบันอุดมศึกษา และผู้เรียน ที่มีกลไกในการส่งเสริม ตรวจสอบ และบังคับใช้ที่มีประสิทธิภาพ นั้น

โดยที่สภามหาวิทยาลัยวลัยลักษณ์เป็นองค์กรสูงสุดที่กำหนดและกำกับนโยบาย ดูแลการบริหารจัดการให้เกิดการปฏิบัติตามนโยบายและพันธกิจมหาวิทยาลัยอย่างมีประสิทธิภาพและเกิดประสิทธิผล เป็นสภาผู้กำกับ (Governing Board) โดยใช้หลักการบริหารจัดการที่ดี “ธรรมัตตาภิบาล” ซึ่งประกอบด้วย (๑) หลักธรรมาภิบาล ๖ หลักการ คือ หลักนิติธรรม หลักคุณธรรม หลักความโปร่งใสตรวจสอบได้ หลักความคุ้มค่า หลักความรับผิดชอบ และหลักการมีส่วนร่วม และ (๒) หลักอัตตาภิบาล ๓ หลักการ คือ ความเป็นอิสระเสรีภาพทางวิชาการ และความรับผิดชอบต่อสังคม ดังนั้น เพื่ออนุวัตรให้เป็นไปตามมาตรา ๒๐ แห่งพระราชบัญญัติการอุดมศึกษา พ.ศ. ๒๕๖๒ และพระราชบัญญัติมาตรฐานทางจริยธรรม พ.ศ. ๒๕๖๒ อาศัยอำนาจตามความในมาตรา ๑๖ (๒) แห่งพระราชบัญญัติมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๓๕ และมติสภามหาวิทยาลัยวลัยลักษณ์ ในการประชุม ครั้งที่ ๒/๒๕๖๕ เมื่อวันที่ ๑๒ กุมภาพันธ์ ๒๕๖๕ โดยคำแนะนำของคณะกรรมการจัดทำข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยประมวลจริยธรรมของนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัย และการพิทักษ์ธรรมาภิบาลของมหาวิทยาลัยวลัยลักษณ์ ในการประชุมครั้งที่ ๓/๒๕๖๔ เมื่อวันที่ ๒๓ กรกฎาคม ๒๕๖๔ จึงออกข้อบังคับไว้ดังต่อไปนี้

ข้อ ๑ ข้อบังคับนี้เรียกว่า “ข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยประมวลจริยธรรมและธรรมาภิบาลนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร ผู้เรียนของมหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๕”

ข้อ ๒ ข้อบังคับนี้ให้ใช้บังคับนับจากวันประกาศเป็นต้นไป

บรรดาระเบียบ ข้อบังคับ หรือประกาศอื่นใดในส่วนที่กำหนดไว้แล้วในข้อบังคับนี้ หรือที่ขัดหรือแย้งกับข้อบังคับนี้ ให้ใช้ข้อบังคับนี้แทน

เมื่อข้อบังคับนี้มีผลบังคับใช้ ให้ยกเลิก

(๑) ประกาศสภามหาวิทยาลัยวลัยลักษณ์ เรื่อง จรรยาบรรณของกรรมการสภามหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๕๔

(๒) ประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง มาตรฐานจริยธรรมและจรรยาบรรณของบุคลากร พ.ศ. ๒๕๕๕

ข้อ ๓ ในข้อบังคับนี้

“มหาวิทยาลัย”	หมายถึง	มหาวิทยาลัยวลัยลักษณ์
“สภามหาวิทยาลัย”	หมายถึง	สภามหาวิทยาลัยวลัยลักษณ์
“นายกสภามหาวิทยาลัย”	หมายถึง	นายกสภามหาวิทยาลัยวลัยลักษณ์
“กรรมการสภามหาวิทยาลัย”	หมายถึง	กรรมการสภามหาวิทยาลัยวลัยลักษณ์
“อธิการบดี”	หมายถึง	อธิการบดีมหาวิทยาลัยวลัยลักษณ์
“ผู้บริหาร”	หมายถึง	อธิการบดี รองอธิการบดี และผู้บริหารของหน่วยงานภายในมหาวิทยาลัยวลัยลักษณ์ทุกระดับ
“บุคลากร”	หมายถึง	ผู้บริหาร พนักงาน และลูกจ้างของมหาวิทยาลัยวลัยลักษณ์ และให้หมายความรวมถึงพนักงานตามสัญญาจ้างด้วย
“ผู้เรียน”	หมายถึง	ผู้ลงทะเบียนศึกษากับมหาวิทยาลัยวลัยลักษณ์
“คณะกรรมการ”	หมายถึง	คณะกรรมการจริยธรรมและพิทักษ์ธรรมาภิบาลมหาวิทยาลัยวลัยลักษณ์
“ประมวลจริยธรรม”	หมายถึง	ประมวลจริยธรรมและธรรมาภิบาลของนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร และผู้เรียนของมหาวิทยาลัยตามที่บัญญัติไว้ในข้อบังคับนี้
“ผลประโยชน์ทับซ้อน”	หมายถึง	การกระทำของผู้ปฏิบัติงานตามอำนาจและหน้าที่ของตน ที่นำเอาผลประโยชน์ส่วนตน หรือส่วนญาติมิตร เข้ามาเกี่ยวข้อง จนส่งผลเสียแก่มหาวิทยาลัย หรือราชการ หรือกระทบต่อจริยธรรมและธรรมาภิบาลตามข้อบังคับนี้

ข้อ ๔ ให้สภามหาวิทยาลัยมีอำนาจวินิจฉัยชี้ขาดปัญหาที่เกิดขึ้นตามข้อบังคับนี้และให้ถือเป็นที่สุด

ให้นายกสภามหาวิทยาลัยรักษาการให้เป็นไปตามข้อบังคับนี้ และให้มีอำนาจออกระเบียบข้อบังคับ คำสั่งใด ๆ ตามมติของสภามหาวิทยาลัย เพื่อให้การปฏิบัติเป็นไปตามข้อบังคับนี้

ลักษณะที่ ๑
บททั่วไป

ข้อ ๕ นายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร และผู้เรียนของมหาวิทยาลัย จะต้องยึดมั่นในประมวลจริยธรรมตามข้อบังคับฉบับนี้

ข้อ ๖ การบริหารงานและการจัดการศึกษาของมหาวิทยาลัยต้องเป็นไปตามมาตรา ๙ แห่งพระราชบัญญัติการอุดมศึกษา พ.ศ. ๒๕๖๒ ตามหลักการดังต่อไปนี้

(๑) หลักความรับผิดชอบต่อสังคม

(๒) หลักเสรีภาพทางวิชาการ

(๓) หลักความเป็นอิสระ

(๔) หลักความเสมอภาค

(๕) หลักธรรมาภิบาล

ลักษณะที่ ๒
ประมวลจริยธรรมและหลักธรรมาภิบาล
ส่วนที่ ๑
ประมวลจริยธรรม

ข้อ ๗ นายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร และบุคลากรของมหาวิทยาลัยมีหน้าที่ต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ของมหาวิทยาลัย มีความเป็นกลางทางการเมือง อำนวยความสะดวกในการให้บริการแก่ประชาชน และต้องประพฤติปฏิบัติตามมาตรฐานทางจริยธรรมของเจ้าหน้าที่ของรัฐ ซึ่งประกอบด้วย

(๑) ยึดมั่นในสถาบันหลักของประเทศ อันได้แก่ ชาติ ศาสนา พระมหากษัตริย์ และการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

(๒) ซื่อสัตย์สุจริต มีจิตสำนึกที่ดี และรับผิดชอบต่อหน้าที่

(๓) กล้าตัดสินใจและกระทำในสิ่งที่ถูกต้องชอบธรรม

(๔) คิดถึงประโยชน์ส่วนรวมมากกว่าประโยชน์ส่วนตัว และมีจิตสาธารณะ

(๕) มุ่งผลสัมฤทธิ์ของงาน

(๖) ปฏิบัติหน้าที่อย่างเป็นธรรมและไม่เลือกปฏิบัติ

(๗) ดำรงตนเป็นแบบอย่างที่ดีและรักษาภาพลักษณ์ของมหาวิทยาลัย

(๘) ไม่ใช้อำนาจข่มขู่ คุกคาม หรือล่วงละเมิดทางเพศต่อผู้อื่น

(๙) ไม่กระทำการอันมีลักษณะขัดแย้งทางผลประโยชน์ของมหาวิทยาลัยอันเกี่ยวเนื่องมาจากการปฏิบัติหน้าที่

ส่วนที่ ๒
หลักธรรมาภิบาล

ข้อ ๘ หลักธรรมาภิบาลของนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร และบุคลากรของมหาวิทยาลัยที่ต้องยึดถือในการปฏิบัติหน้าที่ ต้องเป็นไปตามหลักคุณธรรม หลักนิติธรรม หลักความโปร่งใสตรวจสอบได้ หลักความมีส่วนร่วม หลักความรับผิดชอบ และหลักความคุ้มค่า

ส่วนที่ ๓
จริยธรรมและจรรยาบรรณของนายกสภามหาวิทยาลัย และกรรมการสภามหาวิทยาลัย

ข้อ ๙ นายกสภามหาวิทยาลัย และกรรมการสภามหาวิทยาลัยต้องยึดมั่นตามประมวลจริยธรรมตามข้อ ๗ หลักธรรมาภิบาลตามข้อ ๘ และยังพึงปฏิบัติตนให้เป็นไปตามประกาศอื่นใดของมหาวิทยาลัยที่เกี่ยวข้องโดยอนุโลม

ส่วนที่ ๔
จริยธรรมและจรรยาบรรณของบุคลากร

ข้อ ๑๐ บุคลากรนอกจากต้องยึดมั่นตามประมวลจริยธรรมตามข้อ ๗ และหลักธรรมาภิบาลตามข้อ ๘ แล้ว ยังพึงมีจริยธรรมและจรรยาบรรณ ดังนี้

(๑) ยืนหยัดกระทำในสิ่งที่ถูกต้องและเป็นธรรม

(๒) มีจิตสำนึกที่ดี รับผิดชอบต่อหน้าที่ เสียสละ ปฏิบัติหน้าที่ด้วยความรวดเร็ว โปร่งใส ตรวจสอบได้ และคุ้มค่า

(๓) แยกเรื่องส่วนตัวออกจากตำแหน่งหน้าที่ และยึดถือประโยชน์ส่วนรวมมากกว่าประโยชน์ส่วนตัวและประโยชน์ส่วนบุคคล

(๔) ไม่ใช้ตำแหน่งหน้าที่แสวงหาประโยชน์โดยมิชอบ และไม่กระทำการอันเป็นการขัดกันระหว่างประโยชน์ส่วนตนและประโยชน์ส่วนรวม รวมทั้งกระทำในลักษณะผลประโยชน์ทับซ้อน

(๕) เคารพและปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และมติสภามหาวิทยาลัยอย่างครบถ้วนตรงไปตรงมา

(๖) ปฏิบัติหน้าที่ด้วยความซื่อสัตย์สุจริต เป็นกลางทางการเมือง ให้บริการแก่ประชาชนโดยมีอัธยาศัยที่ดี และมีความเป็นธรรม

(๗) มุ่งผลสัมฤทธิ์ของงาน รักษาคุณภาพและมาตรฐานแห่งวิชาชีพโดยเคร่งครัด

(๘) เป็นแบบอย่างที่ดีในการดำรงตน รักษาชื่อเสียงและภาพลักษณ์ของมหาวิทยาลัยโดยรวม

(๙) ต้องไม่ปฏิบัติงานข้ามขั้นตามลำดับชั้นการบังคับบัญชาโดยไม่ได้รับอนุญาต ไม่ปิดบังซ่อนเร้นข้อราชการอันอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัย รวมทั้งไม่ละเมิดหรือละเว้นการปฏิบัติหน้าที่อันชอบ

(๑๐) ไม่ยินยอมให้ผู้อื่นใช้หน้าที่หรืออำนาจของตนแสวงหาผลประโยชน์อันมิชอบ

(๑๑) ละเว้นการให้สัมภาษณ์ การอภิปราย การปาฐกถา การบรรยาย หรือการวิพากษ์วิจารณ์ในลักษณะเลือกข้าง อันอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัย ราชการ หรือความเป็นกลางทางการเมือง เว้นแต่เป็นการแสดงความคิดเห็นตามหลักวิชาการอันสุจริต

(๑๒) ไม่คัดลอก หรือขโมยผลงานของผู้อื่นมาเป็นของตนโดยเจตนา

(๑๓) ต้องส่งเสริม รักษาชื่อเสียงและภาพลักษณ์ของมหาวิทยาลัย

ข้อ ๑๑ นอกจากข้อบังคับนี้แล้ว บุคลากรพึงประพฤติให้เป็นไปตามประกาศมหาวิทยาลัยวลัยลักษณ์ เรื่อง มาตรฐานจริยธรรมเกี่ยวกับผลประโยชน์ทับซ้อน พ.ศ. ๒๕๖๐ และข้อบังคับ ระเบียบ และประกาศอื่นใดที่เกี่ยวข้องของมหาวิทยาลัย

ข้อ ๑๒ บุคลากรต้องยึดมั่นในการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และจงรักภักดีต่อพระมหากษัตริย์ พระราชินี และพระบรมวงศานุวงศ์

ส่วนที่ ๕
จริยธรรมและจรรยาบรรณของผู้บริหาร

ข้อ ๑๓ ผู้บริหารนอกจากต้องยึดมั่นตามประมวลจริยธรรมตามข้อ ๗ หลักธรรมาภิบาลตามข้อ ๘ และจริยธรรมและจรรยาบรรณของบุคลากรในส่วนที่ ๔ แล้ว ยังพึงมีจริยธรรมและจรรยาบรรณ ดังนี้

(๑) เป็นแบบอย่างหรือผู้นำในการปฏิบัติตนอยู่ในกรอบค่านิยม คุณธรรม จริยธรรมของมหาวิทยาลัย

(๒) เคารพสิทธิในการกระทำหรือการแสดงความคิดเห็นของผู้ใต้บังคับบัญชาที่แสดงออกโดยชอบ

(๓) รักษาเสรีภาพทางวิชาการอย่างมีความรับผิดชอบ

(๔) บริหารจัดการตามหลักบริหารจัดการที่ดี

(๕) ปกป้องและรักษาทรัพย์สินของมหาวิทยาลัย

(๖) บริหารจัดการข้อมูล ความลับของมหาวิทยาลัยด้วยความรอบคอบ

(๗) หลีกเลี่ยงการกระทำในเรื่องของผลประโยชน์ทับซ้อนและข้อผูกพัน

(๘) รับผิดชอบต่อชุมชน สังคม และสิ่งแวดล้อม

(๙) ปกครองผู้อยู่ใต้บังคับบัญชาด้วยความเที่ยงธรรมโดยไม่เห็นแก่ความสัมพันธ์หรือบุญคุณส่วนตัว และส่งเสริมควบคุมให้ผู้อยู่ใต้บังคับบัญชาปฏิบัติตามประมวลจริยธรรมโดยเคร่งครัด

(๑๐) สนับสนุน ส่งเสริม และยกย่องผู้ใต้บังคับบัญชาที่มีความซื่อสัตย์ มีผลงานดีเด่น มีความรู้ความสามารถ และขยันขันแข็ง โดยไม่เลือกปฏิบัติ และยึดมั่นในระบบคุณธรรม

ส่วนที่ ๖
จริยธรรมและจรรยาบรรณของผู้เรียน

ข้อ ๑๔ ผู้เรียนพึงปฏิบัติตนให้เป็นไปตามหลักค่านิยม ๔ ประการ คือ กตัญญู รู้วินัย ใจอาสา และพัฒนาภาวะผู้นำ นอกจากนั้นต้องประพฤติและปฏิบัติตนให้เป็นไปตามข้อบังคับ ระเบียบ และประกาศที่เกี่ยวข้องของมหาวิทยาลัย

ส่วนที่ ๗
จริยธรรมและจรรยาบรรณการตรวจสอบภายใน และการบริหารความเสี่ยง

ข้อ ๑๕ จริยธรรมและจรรยาบรรณการตรวจสอบภายใน และการบริหารความเสี่ยง ให้ยึดถือตามระเบียบมหาวิทยาลัยที่ว่าด้วยการนั้นซึ่งพึงกำหนดขึ้นโดยคำนึงถึงแนวปฏิบัติที่ดีทางวิชาชีพนั้น ๆ ด้วย

ลักษณะที่ ๓
การส่งเสริม ตรวจสอบ และการบังคับใช้ประมวลจริยธรรม
ส่วนที่ ๑
การส่งเสริมและตรวจสอบ

ข้อ ๑๖ นายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย ผู้บริหาร บุคลากร และผู้เรียน มีหน้าที่ส่งเสริมประมวลจริยธรรมและธรรมาภิบาล โดยการเผยแพร่ให้ความรู้ความเข้าใจผ่านกลไกและกระบวนการต่าง ๆ ตามหน้าที่ความรับผิดชอบของตน

ข้อ ๑๗ ในกรณีที่พบว่าบุคลากร หรือผู้เรียนมีวัตรปฏิบัติเชิงจริยธรรมและธรรมาภิบาลอันโดดเด่น สมควรได้รับการยกย่อง สภามหาวิทยาลัยหรืออธิการบดีพึงให้การยกย่องตามสมควร โดยให้เป็นไปตามหลักเกณฑ์ที่กำหนดไว้และประกาศให้บุคลากรและผู้เรียนทราบ

ส่วนที่ ๒
การกำกับดูแลและบังคับใช้

ข้อ ๑๘ ให้สภามหาวิทยาลัยแต่งตั้งคณะกรรมการขึ้นคณะหนึ่ง เรียกว่า “คณะกรรมการจริยธรรมและพิทักษ์ธรรมาภิบาลมหาวิทยาลัยวลัยลักษณ์” จำนวน ๙ คน ประกอบด้วยบุคคลดังต่อไปนี้

(๑) กรรมการสภามหาวิทยาลัยผู้ทรงคุณวุฒิ	เป็นประธานกรรมการ
(๒) กรรมการสภามหาวิทยาลัยผู้ทรงคุณวุฒิ จำนวน ๑ คน	เป็นกรรมการ
(๓) ผู้ทรงคุณวุฒิภายนอกด้านกฎหมาย จำนวน ๑ คน	เป็นกรรมการ
(๔) ผู้ทรงคุณวุฒิภายนอกด้านการบริหารงาน หรือด้านผลประโยชน์ทับซ้อน หรือด้านความโปร่งใส จำนวน ๑ คน	เป็นกรรมการ
(๕) ผู้ทรงคุณวุฒิภายนอกด้านการเงินและการบัญชี จำนวน ๑ คน	เป็นกรรมการ
(๖) ผู้ทรงคุณวุฒิภายนอกด้านบุคคล จำนวน ๑ คน	เป็นกรรมการ
(๗) กรรมการสภามหาวิทยาลัย ซึ่งเลือกจากกรรมการสภาวิชาการ จำนวน ๑ คน	เป็นกรรมการ
(๘) กรรมการสภามหาวิทยาลัย ซึ่งเลือกตั้งจากคณาจารย์ประจำ จำนวน ๑ คน	เป็นกรรมการ
(๙) ผู้แทนพนักงานสายปฏิบัติการวิชาชีพและบริหารทั่วไป จำนวน ๑ คน	เป็นกรรมการ
(๑๐) เลขานุการสภามหาวิทยาลัย	เป็นเลขานุการ
(๑๑) หัวหน้าสำนักงานสภามหาวิทยาลัย	เป็นผู้ช่วยเลขานุการ

ข้อ ๑๙ ประธานกรรมการ และกรรมการ มีวาระการดำรงตำแหน่งคราวละสามปี แต่อาจได้รับการแต่งตั้งใหม่อีกได้

เมื่อครบกำหนดสองปี ให้กรรมการตาม (๒) - (๙) จำนวนสี่คนพ้นจากตำแหน่งโดยวิธีจับสลาก และให้ถือว่าการพ้นจากตำแหน่งโดยการจับสลากดังกล่าวเป็นการพ้นจากตำแหน่งตามวาระ และให้สภามหาวิทยาลัยแต่งตั้งกรรมการขึ้นแทนให้แล้วเสร็จภายในหกสิบวันนับจากวันพ้นจากตำแหน่งโดยการจับสลาก

นอกจากการพ้นจากตำแหน่งตามวาระตามวรรคหนึ่งและวรรคสองแล้ว ประธานกรรมการ และกรรมการ พ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ขาดคุณสมบัติของการเป็นกรรมการในประเภทนั้น

(๔) สภามหาวิทยาลัยมีมติถอดถอนเนื่องจากความประพฤติเสื่อมเสียอย่างร้ายแรงอันส่งผลกระทบชื่อเสียงของมหาวิทยาลัย

(๕) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่ในความผิดอันได้กระทำโดยประมาท หรือความผิดลหุโทษ

(๖) เป็นบุคคลล้มละลาย

(๗) เป็นคนไร้ความสามารถ หรือเสมือนไร้ความสามารถ

ข้อ ๒๐ ให้คณะกรรมการมีอำนาจหน้าที่และความรับผิดชอบ ดังนี้

(๑) ศึกษาวิเคราะห์และเสนอแนะต่อสภามหาวิทยาลัยเพื่อให้การดำเนินการตามข้อบังคับนี้เป็นไปอย่างมีประสิทธิภาพ

(๒) ติดตาม กำกับดูแล ประเมินผลการดำเนินการตามข้อบังคับนี้ และรายงานให้สภามหาวิทยาลัยทราบ

(๓) พิจารณาวินิจฉัยการกระทำของนายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย และบุคลากรที่อาจขัดต่อข้อบังคับนี้

(๔) พิจารณากลั่นกรองเรื่องร้องเรียนต่าง ๆ เกี่ยวกับการละเมิดไม่ปฏิบัติตามข้อบังคับนี้ พร้อมให้ข้อเสนอแนะต่อสภามหาวิทยาลัยพิจารณา

(๕) แต่งตั้งคณะอนุกรรมการ คณะทำงาน หรือบุคคล เพื่อช่วยกระทำการอย่างหนึ่งอย่างใดอันอยู่ในอำนาจหน้าที่ของคณะกรรมการได้ตามความเหมาะสม

(๖) ปฏิบัติหน้าที่อื่นใดตามที่สภามหาวิทยาลัยมอบหมาย

ข้อ ๒๑ การประชุมและการดำเนินการ ให้เป็นไปตามข้อบังคับมหาวิทยาลัยวลัยลักษณ์ ว่าด้วยการประชุมสภามหาวิทยาลัยวลัยลักษณ์ พ.ศ. ๒๕๖๓ หรือที่ออกเพิ่มเติมในภายหลัง หรือการดำเนินการของสภามหาวิทยาลัยโดยอนุโลม

ส่วนที่ ๓
ระบบการบังคับใช้

ข้อ ๒๒ ให้เลขานุการสภามหาวิทยาลัยเป็นผู้พิจารณารับเรื่องและเสนอความเห็นต่อประธานคณะกรรมการ เพื่อพิจารณานำเรื่องเข้าสู่การพิจารณาของคณะกรรมการ

ข้อ ๒๓ ในกรณีที่นายกสภามหาวิทยาลัย กรรมการสภามหาวิทยาลัย บุคลากร กระทำการฝ่าฝืนข้อบังคับนี้ ให้คณะกรรมการดำเนินการไต่สวนและวินิจฉัยให้เป็นไปตามข้อบังคับนี้ โดยให้นำข้อบังคับ ระเบียบ ประกาศ และคำสั่งของมหาวิทยาลัยที่ว่าด้วยการนั้นมาใช้ประกอบการพิจารณาด้วย

ให้คณะกรรมการรายงานผลการไต่สวนและวินิจฉัยให้สภามหาวิทยาลัยพิจารณา โดยคำวินิจฉัยชี้ขาดของสภามหาวิทยาลัยให้ถือเป็นที่สุด

ข้อ ๒๔ ในกรณีที่ผู้เรียนกระทำการฝ่าฝืนข้อบังคับนี้ ให้อธิการบดีหรือผู้ที่อธิการบดีมอบหมายส่งเรื่องให้คณะกรรมการผู้มีอำนาจหน้าที่ดำเนินการไต่สวนและวินิจฉัยให้เป็นไปตามข้อบังคับนี้ โดยให้นำข้อบังคับ ระเบียบ ประกาศ และคำสั่งของมหาวิทยาลัยที่ว่าด้วยการนั้นมาใช้ประกอบการพิจารณาด้วย

ข้อ ๒๕ เมื่อสภามหาวิทยาลัยชี้ขาดผลการไต่สวนและวินิจฉัยแล้ว ปรากฏว่าการกระทำนั้นเข้าข่ายเป็นการกระทำความผิดทางวินัย หรือความผิดทางอาญาร่วมด้วย ให้สภามหาวิทยาลัยส่งเรื่องให้ผู้มีอำนาจหน้าที่ในเรื่องนั้นดำเนินการต่อไป

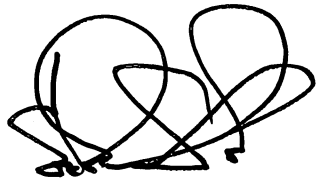
กรณีที่การฝ่าฝืนข้อบังคับนี้ไม่เข้าข่ายการกระทำความผิดทางวินัย หรือความผิดทางอาญา ให้สภามหาวิทยาลัยส่งเรื่องให้ผู้มีอำนาจหน้าที่พิจารณาว่ากล่าวตักเตือน

บทเฉพาะกาล

ข้อ ๒๖ ให้ดำเนินการแต่งตั้งคณะกรรมการภายในเก้าสิบวัน นับแต่วันที่ข้อบังคับนี้มีผลใช้บังคับ

ข้อ ๒๗ ให้มหาวิทยาลัยจัดให้มีการประชาพิจารณ์ข้อบังคับนี้ภายในระยะเวลาหนึ่งปีนับถัดจากวันที่ประกาศใช้

ประกาศ ณ วันที่ ๒๕ กุมภาพันธ์ พ.ศ. ๒๕๖๕



(นายธีระชัย เชมนะสิริ)
นายกสภามหาวิทยาลัยวลัยลักษณ์

ประวัติผู้เขียน

ชื่อ-นามสกุล (ภาษาไทย) นางสาวประไพศรี เหล่าทองมีสกุล
(ภาษาอังกฤษ) Miss Prapaisri Laothongmeesakul

ตำแหน่งและหน่วยงานที่สังกัด

ตำแหน่ง เจ้าหน้าที่วิเคราะห์ระบบงานคอมพิวเตอร์
บุคลากรปฏิบัติการวิชาชีพและบริหารทั่วไป ระดับปฏิบัติการ
สังกัด ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์
เลขที่ 222 ต.ไทยบุรี อ.ท่าศาลา จ.นครศรีธรรมราช 80160
สถานที่ติดต่อ ห้อง 202 อาคารศูนย์คอมพิวเตอร์ มหาวิทยาลัยวลัยลักษณ์
โทรศัพท์ 0-7567-3440, 089-8727355
e-mail lprapais@wu.ac.th, lprapais@mail.wu.ac.th

ประวัติการศึกษา

2533 ปริญญาตรี
วิทยาศาสตร์บัณฑิต (สาขาคณิตศาสตร์)
มหาวิทยาลัยสงขลานครินทร์ จังหวัดสงขลา

ประวัติการอบรม

ประกาศนียบัตร Google Apps. & Facebook for Education,
การสร้างนวัตกรรมเพื่อเพิ่มผลผลิตในการทำงาน,
Customer insight & Service Excellence,
การสร้างและพัฒนาทีมงานเพื่อการพัฒนาองค์กรอย่างยั่งยืน,
WINDOWS NT 4.0 Server Administrator