



สำนักบริหารเทคโนโลยีสารสนเทศ
จุฬาลงกรณ์มหาวิทยาลัย

โครงการจ้างปรับปรุงและติดตั้ง ระบบ Multi-Factor Authentication (MFA)

เอกสารคู่มือการใช้งานสำหรับผู้ใช้งานทั่วไป
(User Manual)

สารบัญ

	หน้า
สารบัญ.....	2
สารบัญภาพ.....	3
Document Control.....	4
1. ข้อมูลทั่วไปของระบบ	5
1.1 การเข้าสู่ระบบ	5
1.2 การออกจากระบบ	6
2. การลงทะเบียนครั้งแรก.....	7
2.1 การเข้าเมนูลงทะเบียนครั้งแรก	7
2.2 การดาวน์โหลดแอปพลิเคชัน Google Authenticator.....	8
2.3 การลงทะเบียนระบบ Multi-Factor Authentication เข้ากับแอปพลิเคชัน Google Authenticator	9
2.4 กรณีที่ QR Code หมดอายุ	13
3. การทดสอบการรับ OTP	14
4. การขอรหัสผ่านชั่วคราว	18

สารบัญภาพ

	หน้า
ภาพที่ 1 เข้าสู่ระบบ	5
ภาพที่ 2 หน้าหลัก.....	5
ภาพที่ 3 ออกจากระบบ	6
ภาพที่ 4 เมนูลงทะเบียนครั้งแรก.....	7
ภาพที่ 5 เมนูแสดงทางเลือกการดาวน์โหลดแอปพลิเคชัน Google Authenticator ตามระบบปฏิบัติการ	7
ภาพที่ 6 QR Code สำหรับดาวน์โหลดแอปพลิเคชัน Google Authenticator	8
ภาพที่ 7 ตัวอย่างกรณีสแกน QR Code ติดตั้งบนอุปกรณ์ iOS.....	8
ภาพที่ 8 เมนูต่อไปหลังจากทำการดาวน์โหลดแอปพลิเคชัน Google Authenticator.....	9
ภาพที่ 9 หน้าจอเพื่อสแกน QR Code สำหรับลงทะเบียนระบบ Multi-Factor Authentication เข้ากับแอปพลิเคชัน Google Authenticator	9
ภาพที่ 10 หน้าจอแอปพลิเคชัน Google Authenticator เมื่อติดตั้งเสร็จแล้ว	10
ภาพที่ 11 เข้าเมนู Scan a QR Code ในแอปพลิเคชัน Google Authenticator เพื่อเปิดกล้อง.....	10
ภาพที่ 12 หน้าจอเมื่อเปิดกล้องเพื่อสแกน QR Code ในระบบ Multi-Factor Authentication ด้วยแอปพลิเคชัน Google Authenticator	11
ภาพที่ 13 หน้าจอแอปพลิเคชัน Google Authenticator เมื่อลงทะเบียนเสร็จเรียบร้อยแล้ว	11
ภาพที่ 14 หน้าจอการยืนยันตัวตน โดยการระบุ OTP ในระบบ Multi-Factor Authentication	12
ภาพที่ 15 การลงทะเบียนสำเร็จ	12
ภาพที่ 16 หน้าจอ QR Code หมดอายุตอนทำการลงทะเบียน	13
ภาพที่ 17 หน้าจอสำหรับการดำเนินการลดอุปกรณ์รับ OTP	14
ภาพที่ 18 หน้าจอยืนยันตัวตน OTP ก่อนลดอุปกรณ์.....	14
ภาพที่ 19 หน้าจอสำหรับกรอกรหัส OTP เพื่อยืนยันตัวตนก่อนลดอุปกรณ์	15
ภาพที่ 20 หน้าจอลดอุปกรณ์รับ OTP.....	15
ภาพที่ 21 หน้าจอการลบอุปกรณ์ที่ได้ทำการลงทะเบียน	16
ภาพที่ 22 หน้าจอยืนยันการลบอุปกรณ์.....	16
ภาพที่ 23 การลบอุปกรณ์สำเร็จ.....	17
ภาพที่ 24 เมนูการขอรหัสผ่านชั่วคราว.....	18
ภาพที่ 25 หน้าจอเมื่อการขอรหัสผ่านชั่วคราวสำเร็จ.....	18
ภาพที่ 26 หน้าจอเมื่อไม่สามารถขอรหัสผ่านชั่วคราวได้.....	19
ภาพที่ 27 อีเมลที่ผู้ใช้งานได้รับเมื่อมีการขอรหัสผ่านชั่วคราว.....	19

Document Control

เอกสารจะถูกปรับปรุงให้ทันสมัย ภายใต้เงื่อนไขต่อไปนี้

1. เมื่อมีการเพิ่มข้อมูลใหม่
2. เมื่อระบบมีการเปลี่ยนแปลงข้อมูลใหม่
3. เมื่อมีการปรับปรุงประจำปี

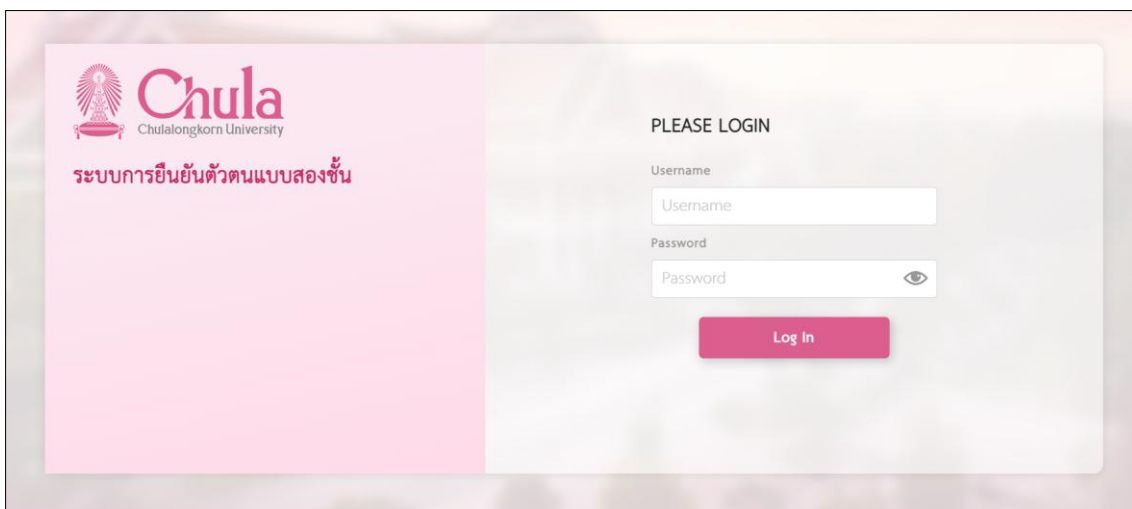
ตารางรายการแก้ไขปรับปรุงเอกสารนี้

วันที่	รายละเอียดการปรับปรุง	ปรับปรุงโดย	ตรวจสอบโดย
22 ธ.ค. 65	Initial Documents	บริษัท ซีนิธคอมพ์ จำกัด	สำนักบริหารเทคโนโลยีสารสนเทศ
23 ธ.ค. 65	ปรับแก้ตามความเห็น คณะกรรมการ	บริษัท ซีนิธคอมพ์ จำกัด	
13 พ.ย. 68	ตรวจสอบเนื้อหา ปรับปรุง ภาษา จัดรูปแบบเอกสาร	สุรติวดี หอกกลาง	

1. ข้อมูลทั่วไปของระบบ

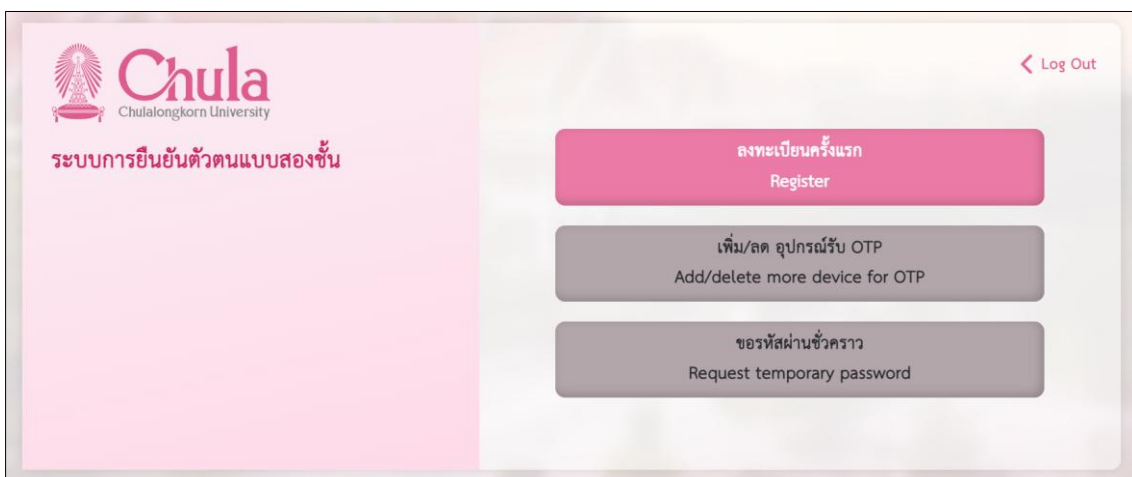
1.1 การเข้าสู่ระบบ

สำหรับผู้ใช้งานที่มีบัญชีผู้ใช้และรหัสผ่าน CUNET Account แล้ว สามารถเข้าสู่ระบบ Multi-Factor Authentication ได้ผ่านทางเว็บไซต์ <https://authenticator.it.chula.ac.th/> ซึ่งรองรับการใช้งานผ่านเว็บเบราว์เซอร์ Google Chrome โดยผู้ใช้งานสามารถกรอกชื่อบัญชีผู้ใช้และรหัสผ่านได้ตามหน้าจอที่ปรากฏในภาพประกอบด้านล่าง



ภาพที่ 1 เข้าสู่ระบบ

เมื่อระบบตรวจสอบความถูกต้องของชื่อผู้ใช้และรหัสผ่านแล้ว ระบบจะนำผู้ใช้งานเข้าสู่หน้าหลักตามภาพประกอบด้านล่าง



ภาพที่ 2 หน้าหลัก

โดยหน้าหลักของระบบประกอบด้วยเมนูทั้งหมด 3 เมนู ดังนี้

1. ลงทะเบียนครั้งแรก (Register)

เมนูนี้สามารถใช้งานได้เฉพาะผู้ใช้งานที่ยังไม่เคยลงทะเบียนขอใช้บริการมาก่อน เมื่อดำเนินการลงทะเบียนเรียบร้อยแล้ว เมนูนี้将无法ใช้งานได้อีก จนกว่าผู้ใช้งานจะลบอุปกรณ์ที่ได้ติดตั้งไว้ทั้งหมดออกก่อน

2. เพิ่ม/ลบ อุปกรณ์รับ OTP (Add/delete more device for OTP)

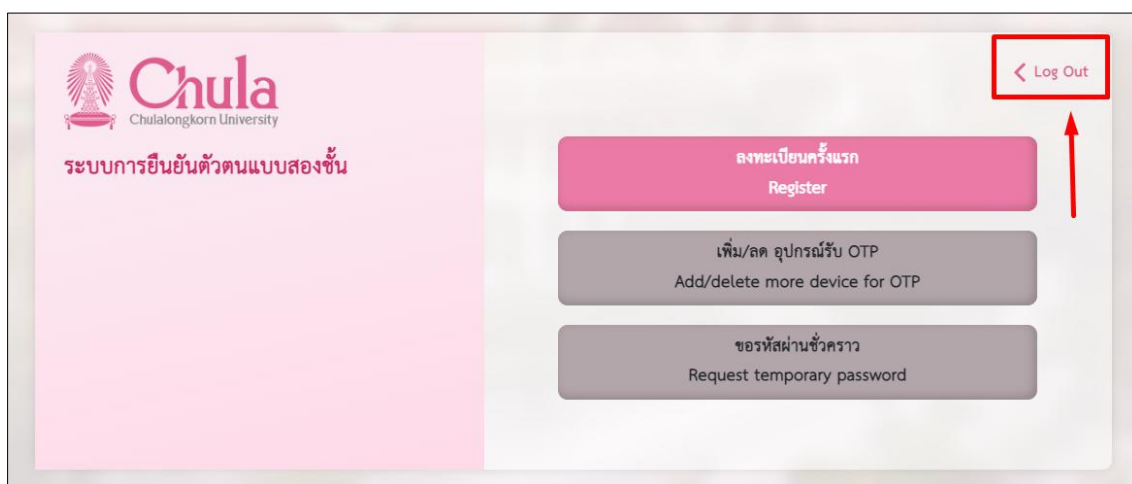
เมนูนี้ใช้สำหรับเพิ่มหรือลบอุปกรณ์ที่ได้ทำการลงทะเบียนไว้ก่อนหน้านี้ โดยผู้ใช้งานจะต้องดำเนินการลงทะเบียนครั้งแรกให้เรียบร้อยก่อน จึงจะสามารถใช้งานเมนูนี้ได้

3. ขอรหัสผ่านชั่วคราว (Request temporary password)

เมนูนี้ใช้สำหรับกรณีที่ผู้ใช้งานลืมหรือไม่สามารถเข้าถึงอุปกรณ์ที่ได้ลงทะเบียนไว้ และต้องการใช้งานรหัส OTP ชั่วคราว ผู้ใช้งานสามารถเข้าเมนูนี้เพื่อขอรหัสผ่านชั่วคราวได้ โดยระบบจะส่งรหัสผ่านดังกล่าวไปยังอีเมลของผู้ใช้งาน ทั้งนี้ ผู้ใช้งานจะต้องดำเนินการลงทะเบียนครั้งแรกให้เรียบร้อยก่อน จึงจะสามารถใช้งานเมนูนี้ได้

1.2 การออกจากระบบ

กรณีต้องการออกจากระบบ ผู้ใช้งานสามารถกดปุ่ม Log out ทางมุมขวาด้านบน ตามภาพประกอบด้านล่าง เพื่อทำการออกจากระบบ

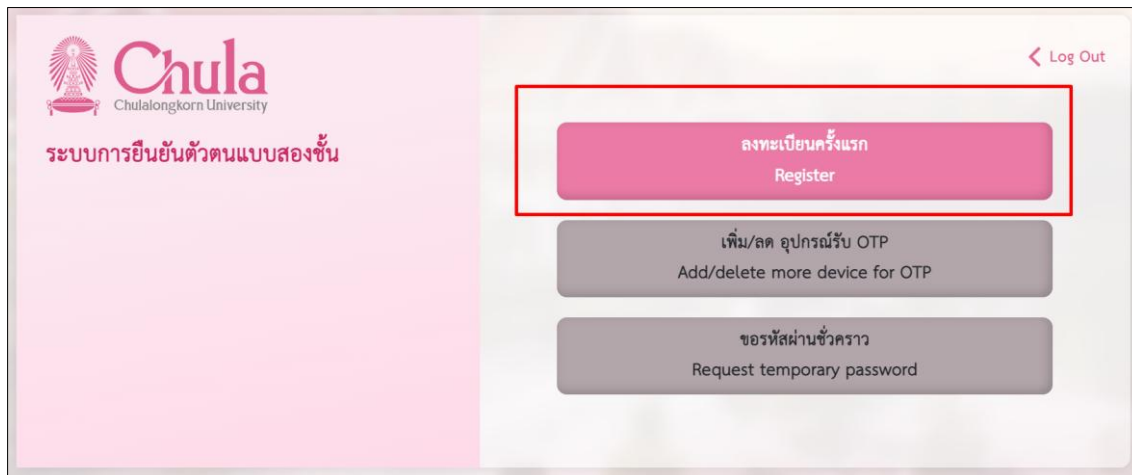


ภาพที่ 3 ออกจากระบบ

2. การลงทะเบียนครั้งแรก

2.1 การเข้าเมนูลงทะเบียนครั้งแรก

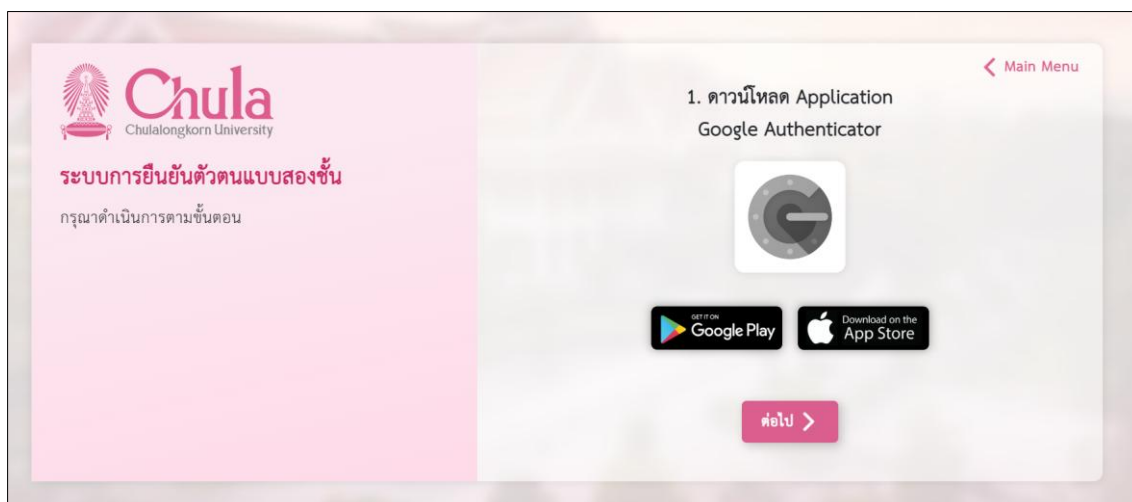
สำหรับผู้ใช้งานที่ยังไม่เคยลงทะเบียนเพื่อใช้งานระบบ Multi-Factor Authentication สามารถดำเนินการลงทะเบียนครั้งแรก ด้วยการกดเลือกปุ่ม ลงทะเบียนครั้งแรก (Register) ได้ตามหน้าจอที่ปรากฏในภาพประกอบด้านล่าง



ภาพที่ 4 เมนูลงทะเบียนครั้งแรก

ระบบจะแสดงหน้าจอช่องทางสำหรับผู้ใช้งานดาวน์โหลดแอปพลิเคชัน Google Authenticator ลงบนอุปกรณ์ที่เตรียมไว้ (Device) โดยแอปพลิเคชัน Google Authenticator รองรับการใช้งานบนระบบปฏิบัติการดังต่อไปนี้

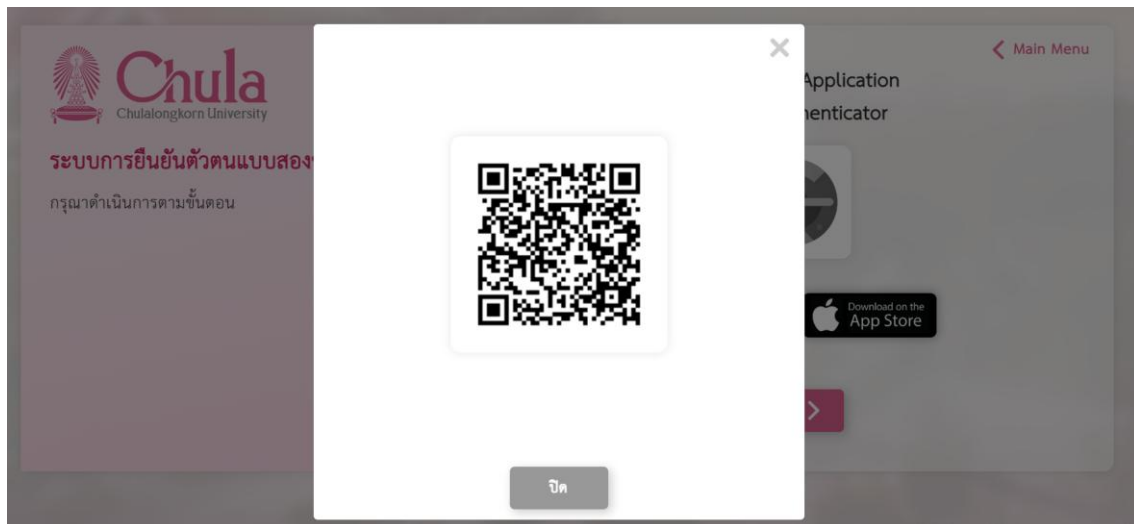
- Android
- iOS



ภาพที่ 5 เมนูแสดงทางเลือกการดาวน์โหลดแอปพลิเคชัน Google Authenticator ตามระบบปฏิบัติการ

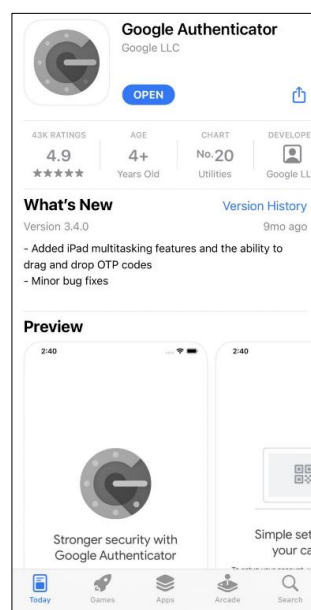
2.2 การดาวน์โหลดแอปพลิเคชัน Google Authenticator

เมื่อผู้ใช้งานเลือกระบบปฏิบัติการของอุปกรณ์ที่ประสงค์จะใช้งานเรียบร้อยแล้ว ระบบจะแสดง QR Code เพื่อนำไปยัง App Store (สำหรับอุปกรณ์ iOS) หรือ Google Play Store (สำหรับอุปกรณ์ Android) เพื่อดาวน์โหลดและติดตั้งแอปพลิเคชัน Google Authenticator ตามภาพประกอบด้านล่าง ทั้งนี้ ผู้ใช้งานสามารถข้ามขั้นตอนการสแกน QR Code และสามารถค้นหาแอปพลิเคชัน Google Authenticator ด้วยตนเองใน App Store หรือ Google Play Store ได้เช่นกัน



ภาพที่ 6 QR Code สำหรับดาวน์โหลดแอปพลิเคชัน Google Authenticator

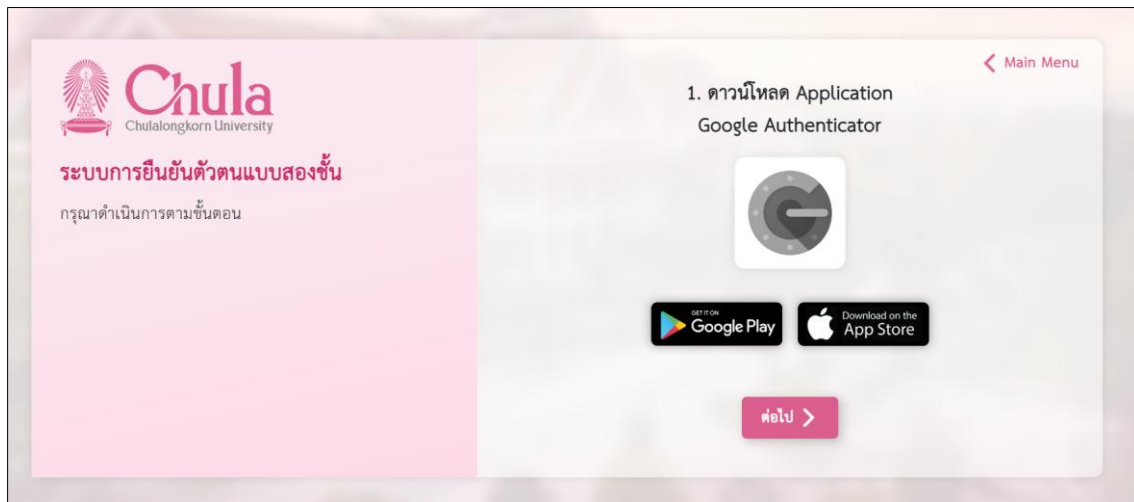
หลังจากที่ผู้ใช้งานสแกน QR Code เรียบร้อยแล้ว ระบบจะแสดงหน้าจอเพื่อเข้าสู่ App Store (สำหรับอุปกรณ์ iOS) หรือ Google Play Store (สำหรับอุปกรณ์ Android) ให้ผู้ใช้งานสามารถเลือกดาวน์โหลดและดำเนินการติดตั้งแอปพลิเคชัน Google Authenticator บนอุปกรณ์ของตน ตามภาพประกอบด้านล่าง



ภาพที่ 7 ตัวอย่างกรณีสแกน QR Code ติดตั้งบนอุปกรณ์ iOS

2.3 การลงทะเบียนระบบ Multi-Factor Authentication เข้ากับแอปพลิเคชัน Google Authenticator

เมื่อผู้ใช้งานติดตั้งแอปพลิเคชัน Google Authenticator เรียบร้อยแล้ว ให้เลือกเมนู **ต่อไป** จากทางด้านล่างของหน้าจอดาวน์โหลดแอปพลิเคชัน Google Authenticator ก่อนหน้านี้ จากนั้นระบบจะนำไปสู่ขั้นตอนการลงทะเบียนระบบ Multi-Factor Authentication เข้ากับแอปพลิเคชัน Google Authenticator ตามภาพประกอบด้านล่าง

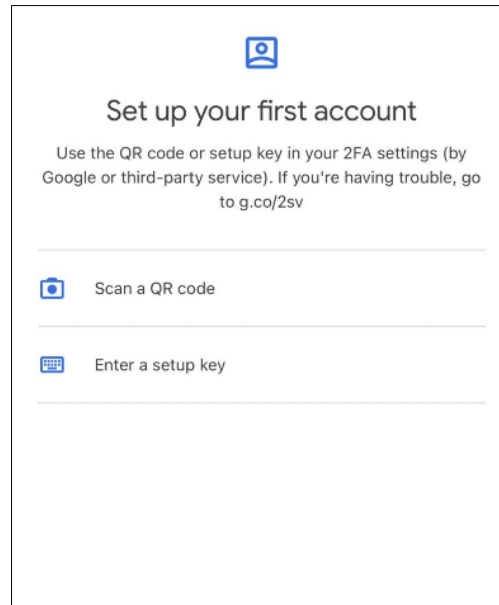


ภาพที่ 8 เมนูต่อไปหลังจากทำการดาวน์โหลดแอปพลิเคชัน Google Authenticator

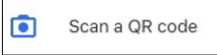


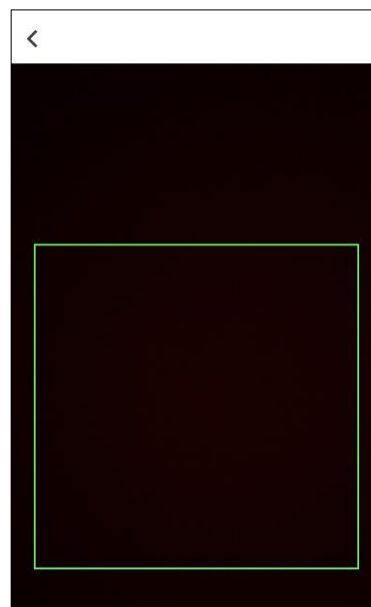
ภาพที่ 9 หน้าจอเพื่อสแกน QR Code สำหรับลงทะเบียนระบบ Multi-Factor Authentication
เข้ากับแอปพลิเคชัน Google Authenticator

เมื่อผู้ใช้งานเปิดแอปพลิเคชัน Google Authenticator บนอุปกรณ์ที่ติดตั้งเรียบร้อยแล้ว จะปรากฏหน้าจอตามภาพประกอบด้านล่าง



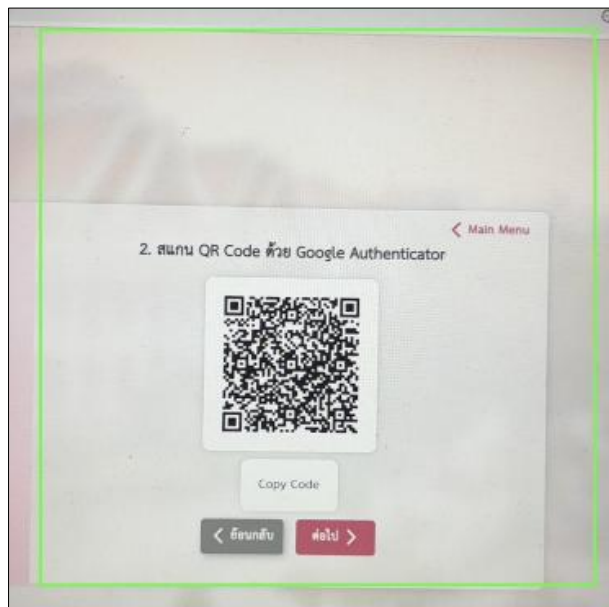
ภาพที่ 10 หน้าจอแอปพลิเคชัน Google Authenticator เมื่อติดตั้งเสร็จแล้ว

หลังจากนั้น ให้ผู้ใช้งานเลือกเมนู  เพื่อทำการลงทะเบียนระบบ Multi-Factor Authentication กับแอปพลิเคชัน Google Authenticator ทั้งนี้ กรณีที่ผู้ใช้งานไม่สามารถสแกน QR Code ได้ ระบบ Multi-Factor Authentication ยังรองรับการคัดลอก Secret Key ด้วยการเลือก  และสามารถลงทะเบียนบัญชีด้วยตนเองผ่านเมนู Enter a setup key



ภาพที่ 11 เข้าเมนู Scan a QR Code ในแอปพลิเคชัน Google Authenticator เพื่อเปิดกล้อง

เมื่อเข้าเมนู Scan a QR Code ในแอปพลิเคชัน Google Authenticator เพื่อเปิดกล้องแล้ว ให้สแกน QR Code ที่ปรากฏในระบบ Multi-Factor Authentication ทั้งนี้ ระบบจะมีเงื่อนไขเรื่องระยะเวลาในการสแกน หากเกินเวลาที่กำหนด ผู้ใช้งานต้องสร้าง QR Code ใหม่ โดยการกดย้อนกลับแล้วเข้ามายังหน้าจอสแกน QR Code ด้วย Google Authenticator อีกครั้ง



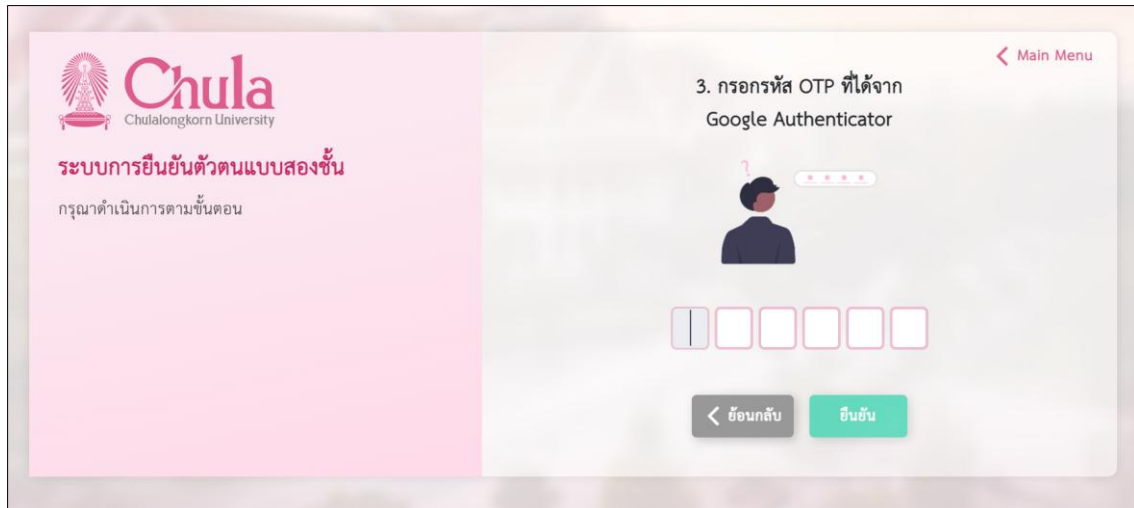
ภาพที่ 12 หน้าจอเมื่อเปิดกล้องเพื่อสแกน QR Code ในระบบ Multi-Factor Authentication ด้วยแอปพลิเคชัน Google Authenticator

เมื่อลงทะเบียนสำเร็จ แอปพลิเคชัน Google Authenticator จะแสดงชื่อระบบและชื่อ Username ที่ผู้ใช้งานใช้ในการลงทะเบียน ตามภาพประกอบด้านล่าง



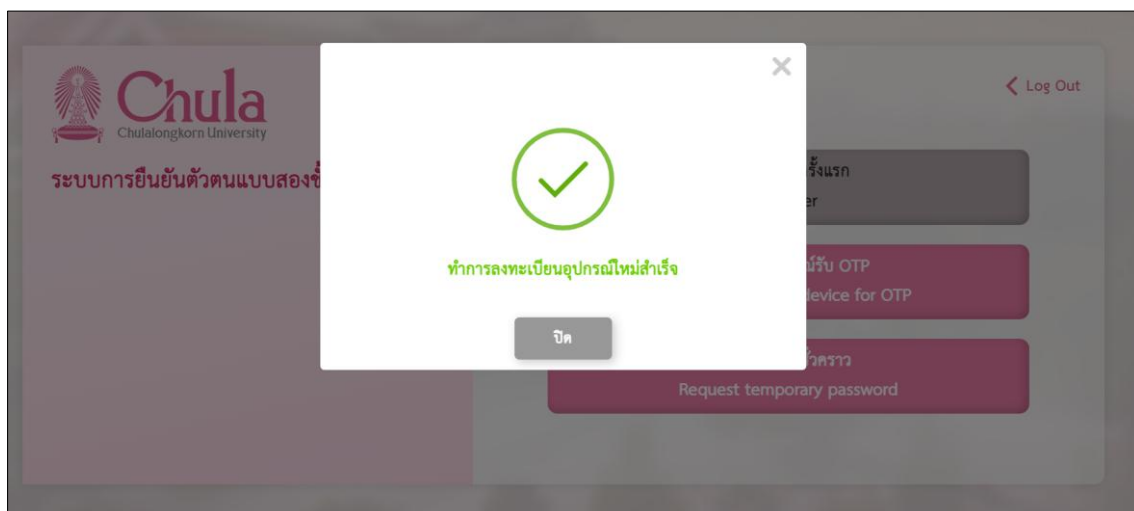
ภาพที่ 13 หน้าจอแอปพลิเคชัน Google Authenticator เมื่อลงทะเบียนเสร็จเรียบร้อยแล้ว

โดยระบบ Multi-Factor Authentication จะแสดงหน้าจอให้ยืนยันการลงทะเบียน โดยให้ผู้ใช้งานระบุ OTP ที่ได้จากแอปพลิเคชัน Google Authenticator จำนวน 6 หลัก



ภาพที่ 14 หน้าจอการยืนยันตัวตน โดยการระบุ OTP ในระบบ Multi-Factor Authentication

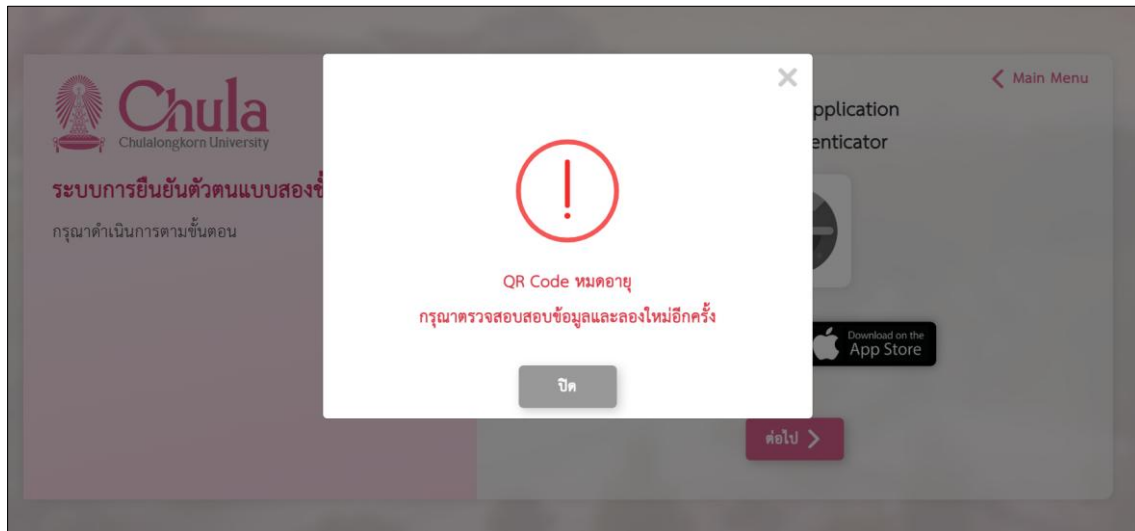
เมื่อระบุ OTP จำนวน 6 หลักที่ได้จากแอปพลิเคชัน Google Authenticator ถูกต้อง ระบบจะแสดงข้อความลงทะเบียนสำเร็จ ตามภาพประกอบด้านล่าง



ภาพที่ 15 การลงทะเบียนสำเร็จ

2.4 กรณีที่ QR Code หมดอายุ

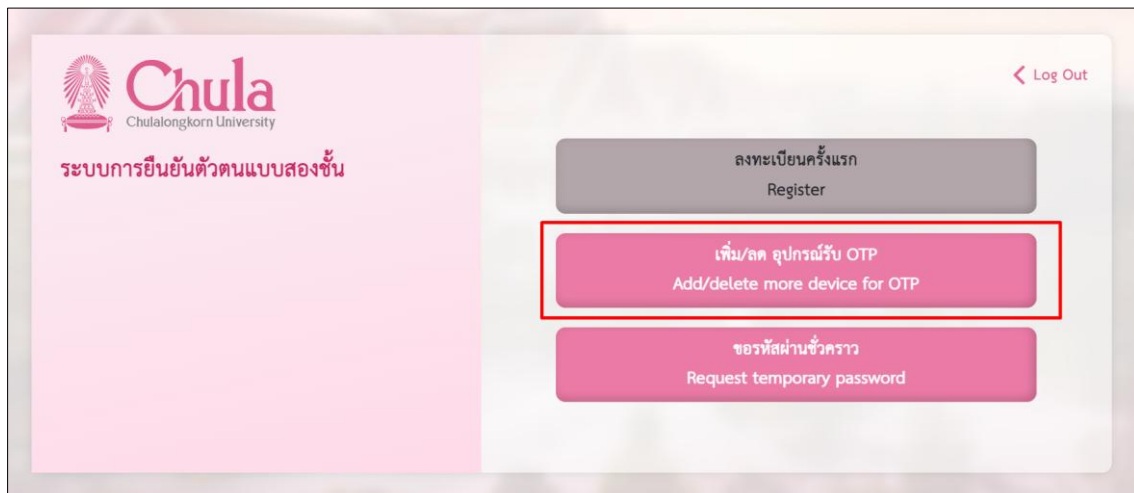
หากผู้ใช้งานใช้เวลานานที่กำหนด ระบบจะแสดงข้อความ QR Code หมดอายุ ตามภาพประกอบด้านล่าง ในกรณีนี้ ผู้ใช้งานต้องสร้าง QR Code ใหม่ โดยการกดย้อนกลับแล้วเข้ามายังหน้าจอ สแกน QR Code ด้วย Google Authenticator อีกครั้ง



ภาพที่ 16 หน้าจอ QR Code หมดอายุตอนทำการลงทะเบียน

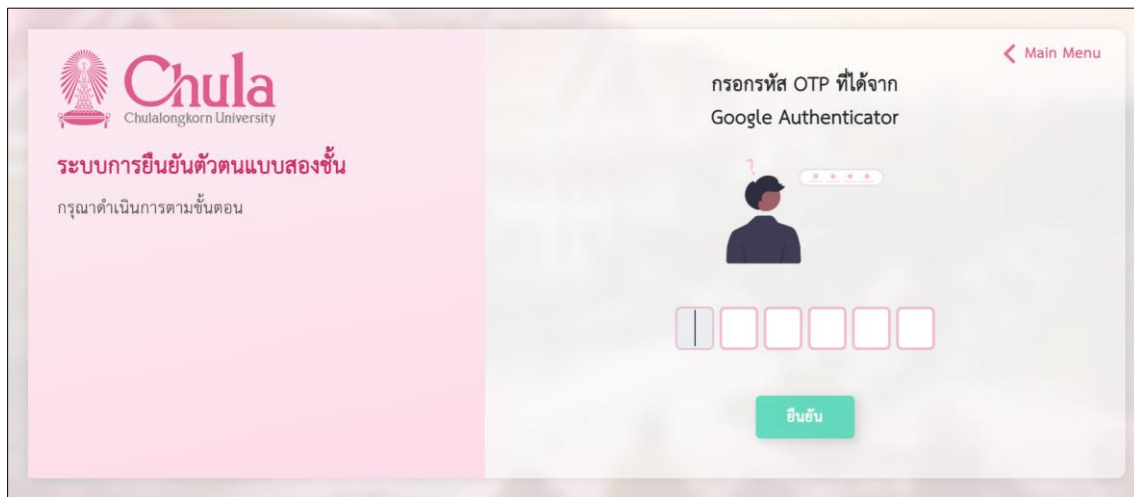
3. การลดอุปกรณ์รับ OTP

เมื่อผู้ใช้งานทำการ Login เข้าสู่ระบบ Multi-Factor Authentication หลังจากที่ได้ดำเนินการลงทะเบียนครั้งแรกเรียบร้อยแล้ว ระบบจะแสดงเมนูการใช้งานที่สามารถเข้าถึงได้ ซึ่งเมนูที่ปรากฏคือ เพิ่ม/ลดอุปกรณ์รับ OTP



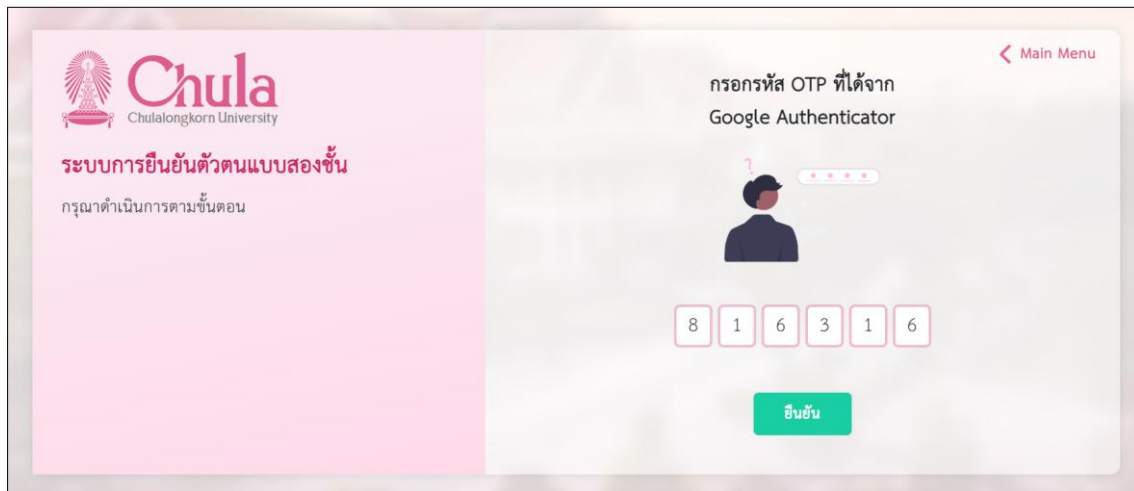
ภาพที่ 17 หน้าจอสำหรับการดำเนินการลดอุปกรณ์รับ OTP

เมื่อเข้าเมนู **เพิ่ม/ลด อุปกรณ์รับ OTP** ระบบจะแสดงหน้าจอให้ยืนยันตัวตน โดยการขอรหัส OTP จำนวน 6 หลักที่ได้จากแอปพลิเคชัน Google Authenticator ตามภาพประกอบด้านล่าง



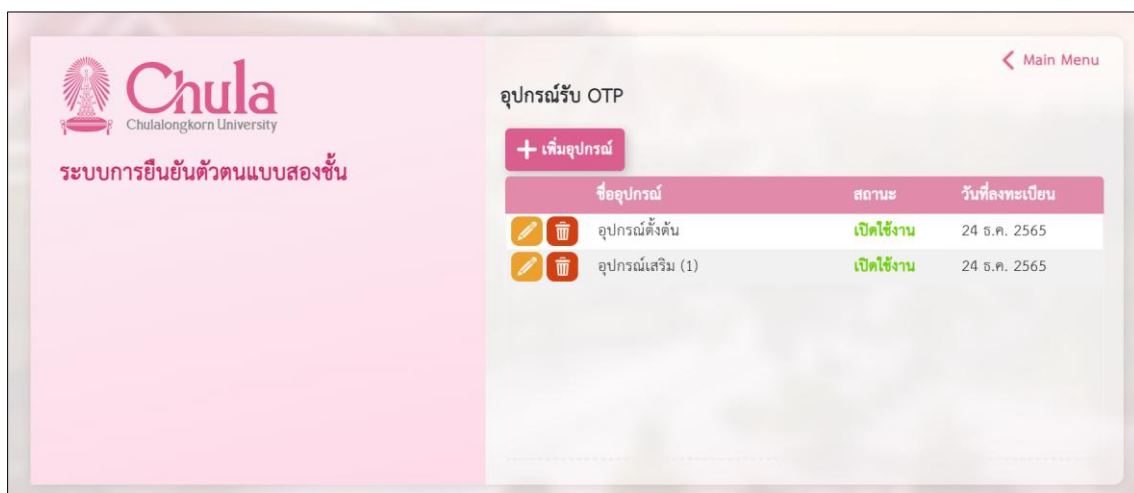
ภาพที่ 18 หน้าจอยืนยันตัวตน OTP ก่อนลดอุปกรณ์

ให้ผู้ใช้งานกรอกรหัส OTP จำนวน 6 หลักที่ได้จากแอปพลิเคชัน Google Authenticator



ภาพที่ 19 หน้าจอสำหรับกรอกรหัส OTP เพื่อยืนยันตัวตนก่อนลดอุปกรณ์

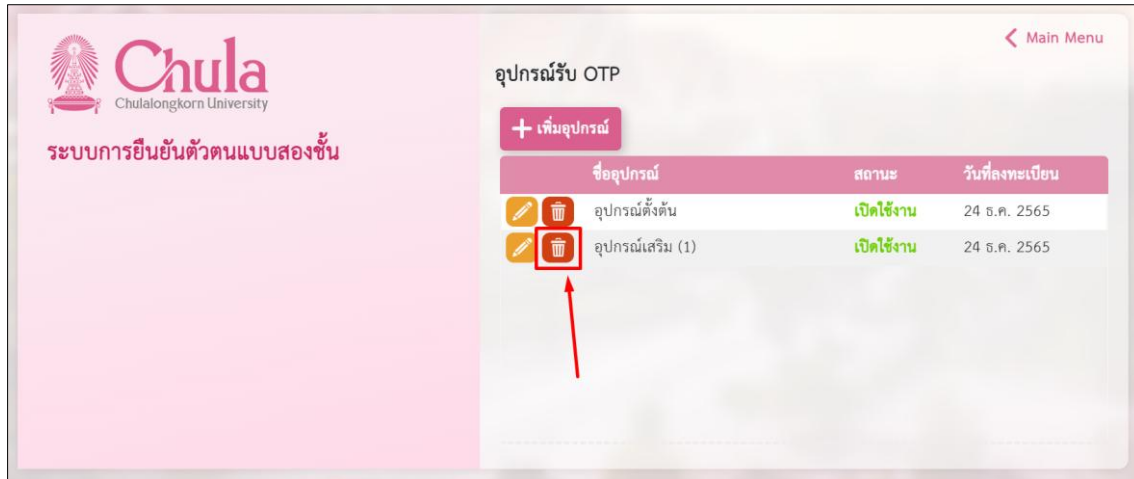
เมื่อผู้ใช้งานกรอกรหัส OTP ถูกต้อง ระบบจะแสดงหน้าจอสำหรับการ ลดอุปกรณ์รับ OTP



ชื่ออุปกรณ์	สถานะ	วันที่ลงทะเบียน
อุปกรณ์ตั้งต้น	เปิดใช้งาน	24 ธ.ค. 2565
อุปกรณ์เสริม (1)	เปิดใช้งาน	24 ธ.ค. 2565

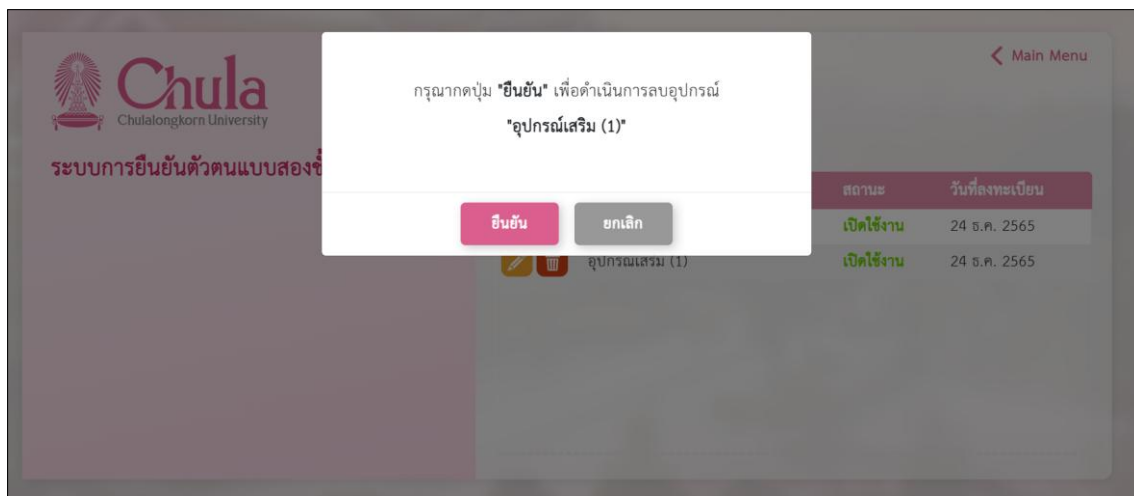
ภาพที่ 20 หน้าจอลดอุปกรณ์รับ OTP

หากผู้ใช้งานประสงค์ที่จะลบอุปกรณ์ที่ใช้ในการรับ OTP ให้คลิกที่  ของอุปกรณ์ที่ต้องการจะลบ การลงทะเบียนออกจากระบบ Multi-Factor Authentication



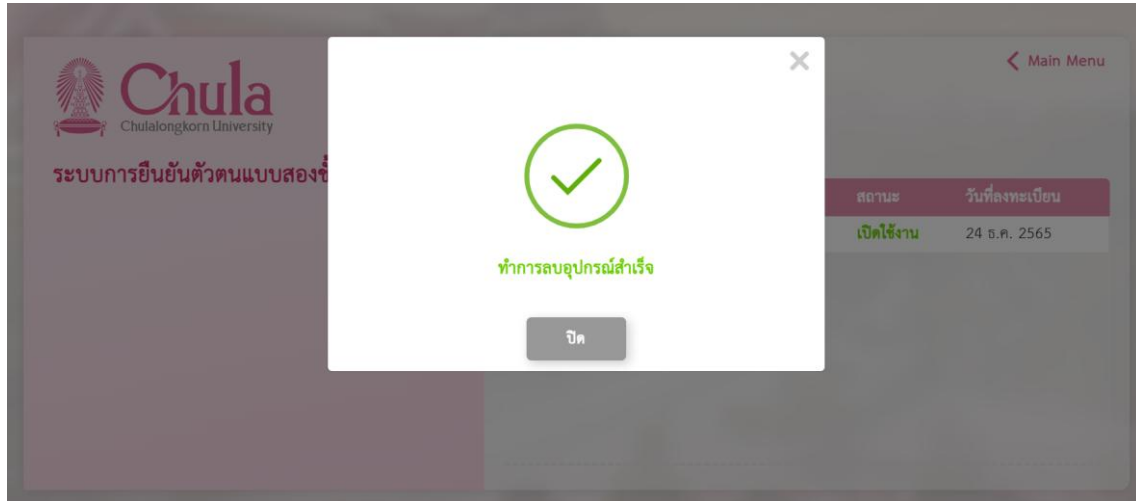
ภาพที่ 21 หน้าจอการลบอุปกรณ์ที่ได้ทำการลงทะเบียน

ระบบจะแสดงหน้าจอให้ผู้ใช้งานยืนยันการลบอุปกรณ์ กรณีที่คลิก  ระบบจะดำเนินการลบอุปกรณ์ที่เลือกออกจากระบบทันที



ภาพที่ 22 หน้าจอยืนยันการลบอุปกรณ์

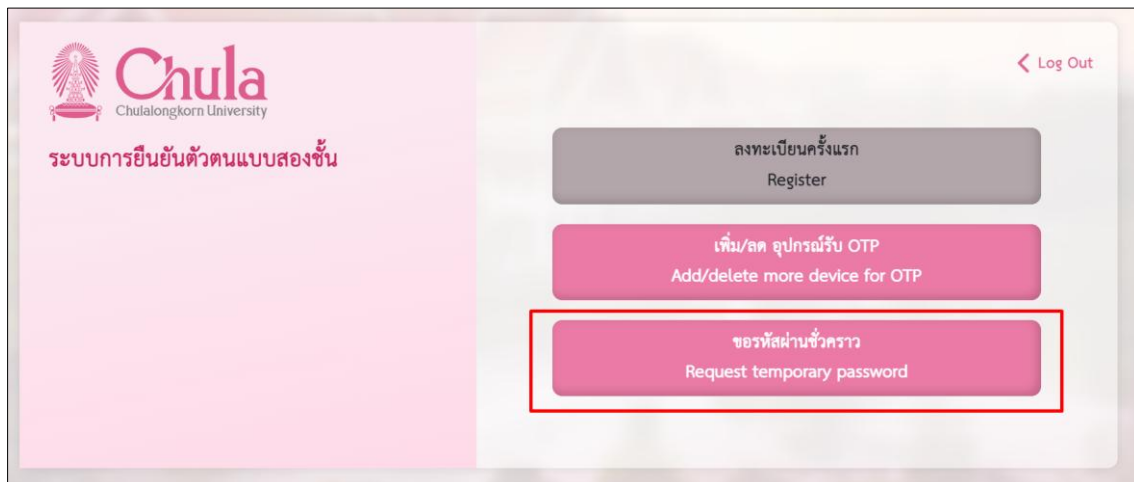
หลังจากนั้น ระบบจะแสดงข้อความยืนยันว่าอุปกรณ์ถูกลบเรียบร้อยแล้ว โดยอุปกรณ์ดังกล่าวจะไม่สามารถใช้ในการยืนยันตัวตนด้วย OTP อีกต่อไป จนกว่าจะทำการลงทะเบียนใหม่



ภาพที่ 23 การลบอุปกรณ์สำเร็จ

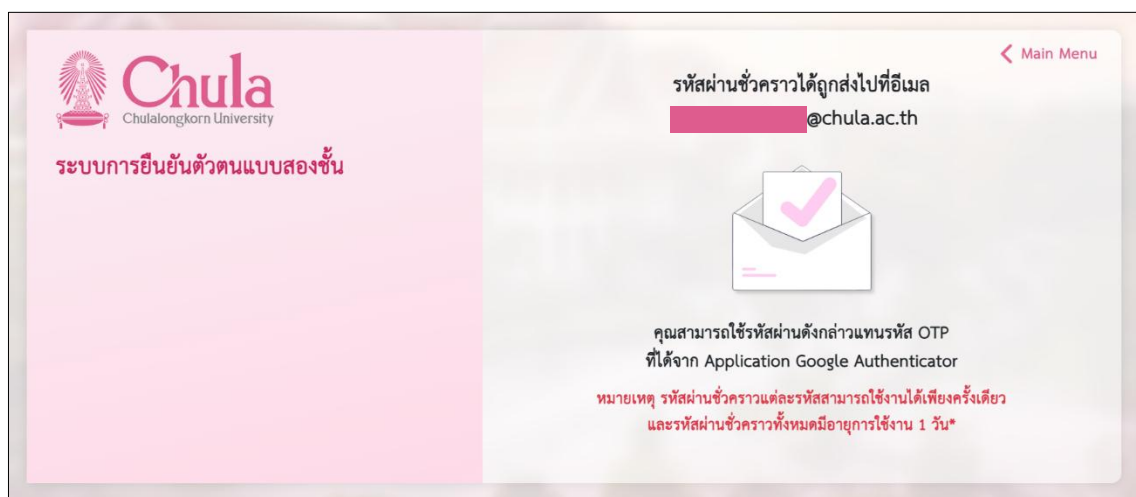
4. การขอรหัสผ่านชั่วคราว

เมื่อผู้ใช้งานทำการ Login เข้าสู่ระบบ Multi-Factor Authentication หลังจากที่ได้ดำเนินการลงทะเบียนครั้งแรกเรียบร้อยแล้ว ระบบจะแสดงเมนูการใช้งานที่สามารถเข้าถึงได้ ซึ่งเมนูที่ปรากฏคือ **ขอรหัสผ่านชั่วคราว**



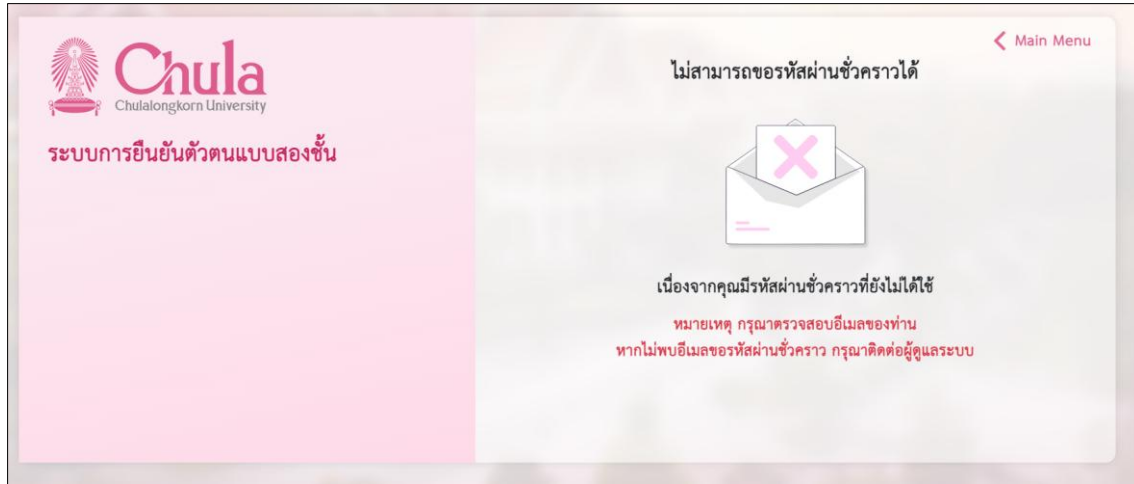
ภาพที่ 24 เมนูการขอรหัสผ่านชั่วคราว

หากผู้ใช้งานประสงค์ที่จะขอรหัสผ่านชั่วคราว ให้คลิกที่ **ขอรหัสผ่านชั่วคราว** เพื่อดำเนินการ โดยระบบจะแสดงหน้าจอยืนยันว่ารหัสผ่านชั่วคราวได้ถูกส่งไปยัง อีเมลของผู้ใช้งานเรียบร้อยแล้ว ตามภาพประกอบด้านล่าง



ภาพที่ 25 หน้าจอเมื่อการขอรหัสผ่านชั่วคราวสำเร็จ

กรณีที่ผู้ใช้งานมีการขอรหัสผ่านชั่วคราวไปแล้ว ระบบจะไม่ให้ขอรหัสผ่านชั่วคราวได้อีก จนกว่าจะครบกำหนดระยะเวลาที่ทางผู้ดูแลระบบกำหนดไว้



ภาพที่ 26 หน้าจอเมื่อไม่สามารถขอรหัสผ่านชั่วคราวได้

เมื่อระบบ Multi-Factor Authentication ส่งรหัสผ่านชั่วคราวไปยังอีเมลของผู้ใช้งานที่ร้องขอ จำนวนรหัสผ่านชั่วคราวที่ได้รับนั้นจะขึ้นอยู่กับข้อกำหนดของผู้ดูแลระบบ ทั้งนี้ รหัสผ่านชั่วคราวแต่ละรหัสสามารถใช้งานได้เพียงครั้งเดียว และรหัสผ่านชั่วคราวทั้งหมดมีอายุการใช้งาน 1 วัน



ภาพที่ 27 อีเมลที่ผู้ใช้งานได้รับเมื่อมีการขอรหัสผ่านชั่วคราว